Installation Guide

Netscape Directory Server

Version 6.2

December 2003

Netscape Communications Corporation ("Netscape") and its licensors retain all ownership rights to the software programs offered by Netscape (referred to herein as "Software") and related documentation. Use of the Software and related documentation is governed by the license agreement for the Software and applicable copyright law.

Your right to copy this documentation is limited by copyright law. Making unauthorized copies, adaptations or compilation works is prohibited and constitutes a punishable violation of the law. Netscape may revise this documentation from time to time without notice.

THIS DOCUMENTATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. IN NO EVENT SHALL NETSCAPE BE LIABLE FOR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND ARISING FROM ANY ERROR IN THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION ANY LOSS OR INTERRUPTION OF BUSINESS, PROFITS, USE, OR DATA.

The downloading, exporting, or reexporting of Netscape software or any underlying information or technology must be in full compliance with all United States and other applicable laws and regulations. Any provision of Netscape software or documentation to the U.S. government is with restricted rights as described in the license agreement for that Software.

Netscape and the Netscape N logo are registered trademarks of Netscape Communications Corporation in the United States and other countries. Other Netscape logos, product names, and service names are also trademarks of Netscape Communications Corporation, which may be registered in some countries. Other product and brand names are the exclusive property of their respective owners.

The Software and documentation are copyright © 2001 Sun Microsystems, Inc. Portions copyright 1999, 2002, 2003 Netscape Communications Corporation. All rights reserved.

==========

Portions of the Software copyright © 1995 PEER Networks, Inc. All rights reserved.

==========

The Software contains the Taligent International Classes from Taligent, Inc. and IBM Corp.

==========

Portions of the Software copyright ©1992-1998 Regents of the University of Michigan. All rights reserved.

==========

The Software contains encryption software from RSA Security Inc. Copyright © 1994 RSA Data Security, Inc. All rights reserved.

This product contains software derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm.

==========

This product incorporates International Components for Unicode (ICU) libraries, ICU is an open source development project sponsored, supported, and used by IBM.

==========

The source code to the Standard Version of Perl can be obtained from CPAN sites, including http://www.perl.com/.

==========

This product incorporates compression code by the Info-ZIP group. There are no extra charges or costs due to the use of this code, and the original compression sources are freely available from http://www.infozip.com/ on the Internet.

==========

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

==========

Portions of the Software copyright © 1989 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms of such U.C. Regents software, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

Portions of the Software copyright (C) 1987, 1988 Student Information Processing Board of the Massachusetts Institute of Technology.

Permission to use, copy, modify, and distribute such M.I.T. software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the names of M.I.T. and the M.I.T. S.I.P.B. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. M.I.T. and the M.I.T. S.I.P.B. make no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Contents

About This Guide 7

Prerequisite Reading 7
Directory Server Overview 7
Conventions Used In This Guide 8
Related Information 9

Chapter 1 Preparing for a Directory Server Installation 11
Installation Components 11
Configuration Decisions 12
Choosing Unique Port Numbers 13
Creating a New Server Root 13
Deciding the User and Group for Your Netscape Servers (UNIX only) 14
Defining Authentication Entities 15
Determining Your Directory Suffix 16
Determining the Location of the Configuration Directory 16
Determining the Location of the User Directory 17
Determining the Administration Domain 18
Installation Process Overview 19
Selecting an Installation Process 19
Migration and Upgrade Process 20
Unpacking the Software 20
Installation Privileges 21

Chapter 2 Using Express and Typical Installation 23
Using Express Installation 23
Using Typical Installation 25
Using Typical Installation on UNIX 25
Using Typical Installation on Windows 29

Chapter 3 Computer System Requirements 33
Summary of Supported Platforms 33
Hardware Requirements 36
Operating System Requirements 36
dsktune Utility 37
HP-UX 11.0 or 11i Operating System 37
Verifying Disk Space Requirements 37
Verifying Required System Modules 38
Installing Patches 38
Tuning the System 39
Installing Third-Party Utilities 40
Microsoft Windows 2000 Advanced Server 41
Configuring a Machine to Run Directory Server 41
Verifying Required System Modules 41
Installing Windows 2000 Server 42
Installing Third-Party Utilities 42
Ensuring System Clock Accuracy 43
Installing Windows Service Packs and Hotfixes 43
Configuring the System Post Installation 43
Red Hat Linux 7.3 Operating System 44
Verifying Disk Space Requirements 44
Verifying Required System Modules 44
Installing System Patches 45
Tuning the System 49
Installing Third-Party Utilities 49
Red Hat Linux Advanced Server 2.1 Operating System 50
Verifying Disk Space Requirements 50
Verifying Required System Modules 50
Installing System Patches 51
Tuning the System 53
Installing Third-Party Utilities 53
Sun Solaris 8 Operating System 54
Verifying Disk Space Requirements 54
Verifying Required System Modules 54
Installing Patches 55
Tuning the System 59
Setting File Descriptors 60
Tuning TCP Parameters 60
Sun Solaris 9 Operating System 61
Verifying Disk Space Requirements 62
Verifying Required System Modules 62
Installing Patches 62
Tuning the System 64

Setting File Descriptors 64
Tuning TCP Parameters 65
DNS and NIS Requirements (UNIX Only) 65

Chapter 4 Silent Installation and Instance Creation 67
Using Silent Installation 67
Preparing Silent Installation Files 68
Sample File for Typical Installation 70
Sample File for Using an Existing Configuration Directory 71
Sample File for Installing the Standalone Netscape Console 72
Specifying Silent Installation Directives 73
Silent Installation File Format 73
[General] Installation Directives 74
[slapd] Installation Directives 75
[admin] Installation Directives 77
[Base] Installation Directives 78
[nsperl] Installation Directives 79
[perldap] Installation Directives 79
Using Silent Instance Creation 79

Chapter 5 Post Installation 83
Launching the Help System 83
Populating the Directory Tree 84

Chapter 6 Migrating and Upgrading From Previous Versions 87
Migration Overview 87
Migration Prerequisites 88
Identifying Custom Schema 90
Migration Procedure 91
Migrating a Standalone Server 92
Migrating a 4.x Replicated Site 99
Migrating a Replicated 4.x Site - Approach 1 100
Migrating a Replicated 4.x Site - Approach 2 101
Migrating a 5.x Replicated Site 103
Migrating a 5.x Multi-Master Deployment 103
Master Migration 104
Hub Migration 104
Consumer Migration 105
Managing Console Fail Over 105
Upgrading From Directory Server 6.x Versions 106
Before You Begin 106
Upgrading 107

After You Upgrade 108

Chapter 7 Uninstalling Directory Server 109
Removing a Directory Server Instance 109
Uninstalling Directory Server 110
Uninstalling the Server on UNIX Systems 110
Uninstalling Directory Server on Windows Systems 111
Using Directory Server's Uninstall Utility 111
Using Windows Add/Remove Programs Utility 112

Chapter 8 Troubleshooting 115
Running dsktune 115
Common Installation Problems 119

Glossary 123

Index 139

About This Guide

Welcome to Netscape Directory Server (Directory Server). This manual provides a high-level overview of design and planning decisions you need to make before installing the Directory Server, and describes the different installation methods that you can use.

This preface contains the following sections:

- Prerequisite Reading (page 7)
- Directory Server Overview (page 7)
- Conventions Used In This Guide (page 8)
- Related Information (page 9)

Prerequisite Reading

Before you install Directory Server, we recommend that you read the *Netscape Directory Server Deployment Guide*. This guide covers key concepts on how to design and plan your directory service.

After you finish planning your directory service, follow the steps in this installation guide to install the Directory Server and its related software components.

Directory Server Overview

The major components of Directory Server include:

- **An LDAP server**—The core of the directory service, provided by the `ns-slapd` daemon, and compliant with the LDAP v3 Internet standards.

- **Directory Server Console**—An improved management console that dramatically reduces the effort of setting up and maintaining your directory service. The directory console is part of Netscape Console, the common management framework for Netscape servers.
- **SNMP Agent**—Permits you to monitor your directory server in real time using the Simple Network Management Protocol (SNMP).
- **Online backup and restore**—Allows you to create backups and restore from backups while the server is running.

Conventions Used In This Guide

This section explains the conventions used in this book.

`Monospaced` font—This typeface is used for any text that appears on the computer screen or text that you should type. It is also used for filenames, functions, and examples.

NOTE	Notes and Cautions mark important information. Make sure you read the information before continuing with a task.

The greater than symbol (>) is used as a separator for successive menu selections. For example, Object > New > User means that you should pull down the Object menu, drag the mouse down to highlight New, and drag the mouse across to the New submenu in which you must select User.

Throughout this book you will see path references of the form:

serverRoot`/slapd-`*serverID*`/...`

serverRoot is the installation directory. On UNIX, `/usr/netscape/servers` is the default installation directory. On Windows, `c:\netscape\servers` is the default installation directory. If you have installed Directory Server in a different location, you should adapt the path accordingly.

serverID is the ID or identifier you assigned to an instance of Directory Server when you installed it. For example, if you gave the server an identifier of `phonebook`, then the actual path would look like this: `/usr/netscape/servers/slapd-phonebook/. . .`

All paths specified in this manual are in UNIX format. If you are using a Windows-based Directory Server, you should assume the equivalent file paths whenever UNIX file paths are shown in this guide.

Related Information

The document set for Directory Server also contains the following guides:

- *Netscape Directory Server Administrator's Guide*. Contains procedures for the day-to-day maintenance of your directory service. Includes information on configuring server-side plug-ins.
- *Netscape Directory Server Deployment Guide*. Contains procedures for the day-to-day maintenance of your directory service. Includes information on configuring server-side plug-ins.
- *Netscape Directory Server Configuration, Command, and File Reference*. Contains information about using the command-line scripts shipped with Directory Server.
- *Netscape Directory Server Schema Reference*. Contains information about the Directory Server schema.
- *Netscape Directory Server Plug-In Programmer's Guide*. Describes how to write server plug-ins in order to customize and extend the capabilities of Directory Server.

For a list of documentation installed with Directory Server, open this file:

serverRoot`/manual/en/slapd/index.htm`

For the latest information about Directory Server, including current release notes, complete product documentation, technical notes, and deployment information, check this site:

`http://enterprise.netscape.com/docs`

Chapter 1

Preparing for a Directory Server Installation

Before you begin installing Netscape Directory Server (Directory Server), you should have an understanding of the various Directory Server components and the design and configuration decisions you need to make.

To help you prepare for your Directory Server installation, you should be familiar with the concepts contained in the following sections:

- Installation Components (page 11)
- Configuration Decisions (page 12)
- Installation Process Overview (page 19)
- Installation Privileges (page 21)

The *Netscape Directory Server Deployment Guide* contains basic directory concepts as well as guidelines to help you design and successfully deploy your directory service. Be sure you understand the concepts presented in this manual before proceeding with the installation process.

Installation Components

Directory Server contains the following software components:

- **Netscape Console**—Netscape Console provides the common user interface for all Netscape server products. From it you can perform common server administration functions such as stopping and starting servers, installing new server instances, and managing user and group information. Netscape Console can be installed as a stand-alone application on any machine. You can also install it on your network and use it to manage remote servers.

- **Netscape Administration Server**—Administration Server is a common front-end to all Netscape servers. It receives communications from Netscape Console and passes those communications on to the appropriate Netscape server. Your site will have at least one Administration Server for each server root in which you have installed an Netscape server.
- **Directory Server**—Directory Server is Netscape's LDAP implementation. The Directory Server runs as the `ns-slapd` process (on UNIX) or `slapd` service (on Windows). This is the server that manages the directory databases and responds to client requests. Directory Server is a required component.

The order in which you install and configure the various components depends on whether you are performing a new installation or an upgrade. See "Installation Process Overview," on page 19 for details.

Configuration Decisions

During Directory Server installation, you are prompted for basic configuration information. Decide how you are going to configure these basic parameters before you begin the installation process. You are prompted for some or all of following information, depending on the type of installation that you decide to perform:

- Port number; see "Choosing Unique Port Numbers," on page 13.
- Server root; see "Creating a New Server Root," on page 13.
- Users and groups to run the server as; see "Deciding the User and Group for Your Netscape Servers (UNIX only)," on page 14.
- Your directory suffix; see "Determining Your Directory Suffix," on page 16.
- Several different authentication user IDs; see "Defining Authentication Entities," on page 15.
- The location of the configuration and user Directory Servers; see "Determining the Location of the Configuration Directory," on page 16 and "Determining the Location of the User Directory".
- The administration domain; see "Determining the Administration Domain," on page 18.

Choosing Unique Port Numbers

Port numbers can be any number from 1 to 65535. Keep the following in mind when choosing a port number for your Directory Server:

- The standard Directory Server (LDAP) port number is 389.
- Port 636 is reserved from LDAP over SSL. Therefore, do not use port number 636 for your standard LDAP installation, even if 636 is not already in use. You can also use LDAP over TLS on the standard LDAP port.
- Port numbers between 1 and 1024 have been assigned to various services by the Internet Assigned Numbers Authority. Do not use port numbers below 1024 other than 389 or 636 for directory services as they will conflict with other services.
- On UNIX platforms, Directory Server must be run as `root` if it will listen on either port 389 or 636.
- On Windows platforms, the directory service must have `administrative` privileges if it will use ports 389 or 636.
- Make sure the ports you choose are not already in use. Additionally, if you are using both LDAP and LDAPS communications, make sure the port numbers chosen for these two types of access are not identical.

For information on how to set up LDAP over SSL (LDAPS) for Directory Server, see the *Netscape Directory Server Administrator's Guide.*

Creating a New Server Root

Your server root is the directory where you install your Netscape servers. The default server root for Directory Server is `/usr/netscape/servers`.

The server root must meet the following requirements:

- The server root must be a directory on a local disk drive; you cannot use a networked drive for installation purposes. The file sharing protocols such as AFS, NFS, and SMB do not provide file locking and performance suitable for use by the Directory Server. The server database index files may be damaged if they are not held on a local file system.
- The directory must not already exist or must be empty.
- The server root directory must not be the same as the directory from which you are running the `setup` program.

By default, the server root directory is one of the following:

- `/usr/netscape/servers` (on UNIX systems)
- `c:\netscape\servers` (on Windows systems)

Deciding the User and Group for Your Netscape Servers (UNIX only)

For security reasons, it is always best to run UNIX-based production servers with normal user privileges. That is, you do not want to run Directory Server with `root` privileges. However, you will have to run Directory Server with root privileges if you are using the default Directory Server ports. If Directory Server is to be started by Administration Server, Administration Server must run either as `root` or as the same user as Directory Server.

You must therefore decide what user accounts you will use for the following purposes:

- The user and group under which you will run Directory Server.

  If you will not be running the Directory Server as `root`, it is strongly recommended that you create a user account for all Netscape servers. You should not use any existing operating system account, and must not use the `nobody` account. Also you should create a common group for the directory server files; again, you must not use the `nobody` group.

- The user and group under which you will run Administration Server.

  For installations that use the default port numbers, this must be `root`. However, if you use ports over 1024, then you should create a user account for all Netscape servers, and run Administration Server as this account.

  As a security precaution, when Administration Server is being run as `root`, it should be shut down when it is not in use.

You should use a common group for all Netscape servers, such as `gid Netscape`, to ensure that files can be shared between servers when necessary.

Before you can install Directory Server and Administration Server, you must make sure that the user and group accounts you will use exist on your system.

Defining Authentication Entities

As you install Directory Server and Administration Server, you will be asked for various user names, distinguished names (DN), and passwords. This list of login and bind entities will differ depending on the type of installation that you are performing:

- Directory Manager DN and password.

  The Directory Manager DN is the special directory entry to which access control does not apply. Think of the directory manager as your directory's superuser. (In former releases of Directory Server, the Directory Manager DN was known as the *root DN*).

  The default Directory Manager DN is `cn=Directory Manager`. Because the Directory Manager DN is a special entry, the Directory Manager DN does not have to conform to any suffix configured for your Directory Server. Therefore, you must not manually create an actual Directory Server entry that has the same DN as the directory manager DN.

  The Directory Manager password must be at least 8 characters long, and is limited to ASCII letters, digits, and symbols.

- Configuration Directory Administrator ID and password.

  The configuration directory administrator is the person responsible for managing all the Netscape servers accessible through Netscape Console. If you log in with this user ID, then you can administer any Netscape server that you can see in the server topology area of Netscape Console.

  For security, the configuration directory administrator should not be the same as the directory manager. The default configuration directory administrator ID is `admin`.

- Administration Server User and password.

  You are prompted for this only during custom installations. The Administration Server user is the special user that has all privileges for the local Administration Server. Authentication as this person allows you to administer all the Netscape servers stored in the local server root.

  Administration Server user ID and password is used only when the Directory Server is down and you are unable to log in as the configuration directory administrator. The existence of this user ID means that you can access Administration Server and perform disaster recovery activities such as starting Directory Server, reading log files, and so forth.

Normally, Administration Server user and password should be identical to the configuration directory administrator ID and password.

Determining Your Directory Suffix

A directory suffix is the directory entry that represents the first entry in a directory tree. You will need at least one directory suffix for the tree that will contain your enterprise's data. It is common practice to select a directory suffix that corresponds to the DNS host name used by your enterprise. For example, if your organization uses the DNS name `example.com`, then select a suffix of `dc=example,dc=com`.

For more information on planning the suffixes for your directory service, see the *Netscape Directory Server Deployment Guide*.

Determining the Location of the Configuration Directory

Many Netscape servers, including Directory Server, use an instance of Directory Server to store configuration information. This information is stored in the `o=NetscapeRoot` directory tree. It does not need to be held on the same Directory Server as your directory data. Your *configuration directory* is the Directory Server that contains the `o=NetscapeRoot` tree used by your Netscape servers.

If you are installing Directory Server only to support other Netscape servers, then that Directory Server is your configuration directory. If you are installing Directory Server to use as part of a general directory service, then you will have multiple Directory Servers installed in your enterprise and you must decide which one will host the configuration directory tree, `o=NetscapeRoot`. You must make this decision before you install any Netscape servers (including Directory Server).

For ease of upgrades, you should use a Directory Server instance that is dedicated to supporting the `o=NetscapeRoot` tree; this server instance should perform no other function with regard to managing your enterprise's directory data. Also, do not use port 389 for this server instance because doing so could prevent you from installing a Directory Server on that host that can be used for management of your enterprise's directory data.

Because the configuration directory normally experiences very little traffic, you can allow its server instance to coexist on a machine with another more heavily loaded Directory Server instance. However, for very large sites that are installing a large number of Netscape servers, you may want to dedicate a low-end machine to the configuration directory so as to not hurt the performance of your other production servers. Netscape server installations result in write activities to the configuration directory. For large enough sites, this write activity could result in a short-term performance hit to your other directory activities.

Also, as with any directory installation, consider replicating the configuration directory to increase availability and reliability. See the *Netscape Directory Server Deployment Guide* for information on using replication and DNS round robins to increase directory availability.

CAUTION Corrupting the configuration directory tree can result in the necessity of reinstalling all other Netscape servers that are registered in that configuration directory. Remember the following guidelines when dealing with the configuration directory:

- Always back up your configuration directory after you install a new Netscape server.
- Never change the host name or port number used by the configuration directory.
- Never directly modify the configuration directory tree. Only the `setup` program for the various Netscape servers should ever modify the configuration.

Determining the Location of the User Directory

Just as the configuration directory is the Directory Server that is used for Netscape server administration, the *user directory* is the Directory Server that contains the entries for users and groups in your enterprise.

For most directory installations, the user directory and the configuration directory should be two separate server instances. These server instances can be installed on the same machine, but for best results you should consider placing the configuration directory on a separate machine.

Between your user directory and your configuration directory, it is your user directory that will receive the overwhelming percentage of the directory traffic. For this reason, you should give the user directory the greatest computing resources. Because the configuration directory should receive very little traffic, it can be installed on a machine with very low-end resources (such as a minimally-equipped Pentium).

Also, you should use the default directory ports (389 and 636) for the user directory. If your configuration directory is managed by a server instance dedicated to that purpose, you should use some non-standard port for the configuration directory.

You cannot install a user directory until you have installed a configuration directory somewhere on your network.

Determining the Administration Domain

The administration domain allows you to logically group Netscape servers together so that you can more easily distribute server administrative tasks. A common scenario is for two divisions in a company to each want control of their individual Netscape servers. However, you may still want some centralized control of all the servers in your enterprise. Administration domains allow you to meet these conflicting goals.

Administration domains have the following qualities:

- All servers share the same configuration directory, regardless of the domain they belong to.
- Servers in two different domains may use two different user directories for authentication and user management.
- The configuration directory administrator has complete access to all installed Netscape servers, regardless of the domain that they belong to.
- Each administration domain can be configured with an administration domain owner. This owner has complete access to all the servers in the domain but does not have access to the servers in any other administration domain.
- The administration domain owner can grant individual users administrative access on a server by server basis within the domain.

For many installations, you can have just one administration domain. In this case, choose a name that is representative of your organization. For other installations, you may want different domains because of the demands at your site. In the latter case, try to name your administration domains after the organizations that will control the servers in that domain.

For example, if you are an ISP and you have three customers for whom you are installing and managing Netscape servers, create three administration domains each named after a different customer.

Installation Process Overview

You can use one of several installation processes to install Directory Server. Each one guides you through the installation process and ensures that you install the various components in the correct order.

The sections that follow outline the installation processes available, how to upgrade from an earlier release of Directory Server, and how to unpack the software to prepare for installation.

Selecting an Installation Process

You can install Directory Server software using one of the four different installation methods provided in the `setup` program:

- **Express Installation**. Use this if you are installing for the purposes of evaluating or testing Directory Server. Express installation is described in “Using Express Installation,” on page 23.
- **Typical Installation**. Use this if you are performing a normal installation of Directory Server. Typical installation is described in “Using Typical Installation,” on page 25.
- **Custom Installation.** In Directory Server 6.x, the custom installation process is very similar to the typical installation process. The main difference is that the custom installation process allows you to import an LDIF file to initialize the user directory database that is created by default.
- **Silent Installation**. Use this if you want to script your installation process. This is especially useful for installing multiple consumer servers around your enterprise. Silent install is described in Chapter 4, “Silent Installation and Instance Creation.”

Beyond determining which type of installation process you will use, the process for installing Directory Server is as follows:

1. Plan your directory service. By planning your directory tree in advance, you can design a service that is easy to manage and easy to scale as your organization grows. For guidance on planning your directory service, refer to the *Netscape Directory Server Deployment Guide*.
2. Install your Directory Server as described in this manual.
3. Create the directory suffixes and databases. You do not have to populate your directory now; however, you should create the basic structure for your tree, including all major roots and branch points. For information about the different methods of creating a directory entry, refer to the *Netscape Directory Server Administrator's Guide.*
4. Create additional Directory Server instances and set up replication agreements between your directory servers to ensure availability of your data.

Migration and Upgrade Process

Directory Server supports migration and upgrade from previous releases of Directory Server. The migration and upgrade processes are described in Chapter 6, "Migrating and Upgrading From Previous Versions."

For information on migrating servers involved in replication agreements, refer to the *Netscape Directory Server Administrator's Guide*.

Unpacking the Software

If you have obtained Directory Server software from the web site, you will need to unpack it before beginning installation.

1. Create a new directory for the installation:

   ```
   # mkdir ds
   # cd ds
   ```

2. Download the product binaries file to the installation directory.
3. On UNIX, unpack the product binaries file using the following command:

   ```
   # gzip -dc filename.tar.gz | tar -xvof -
   ```

   where *filename* corresponds to the product binaries that you want to unpack.

On Windows, unzip the product binaries.

Installation Privileges

On UNIX you must install as `root` if you choose to run the server on a port below 1024, such as the default LDAP ports: 389 and 636 (LDAP over SSL). If you choose port numbers higher than 1024, you can install using any valid UNIX login. On Windows, you must run the installation as `administrator`.

Chapter 2

Using Express and Typical Installation

This chapter describes how to perform basic installation activities. This chapter contains the following sections:

- Using Express Installation (page 23)
- Using Typical Installation (page 25)

Using Express Installation

Use express installation if you are installing Directory Server to evaluate or test the product. Because express installation does not offer you the choice of selecting your server port number or your directory suffix, you should not use it for production installations.

To perform an express installation, do the following:

1. On UNIX machines, log in as `root` (root login is required for express installation). On Windows machines, log in with administrator privileges.
2. Create a new directory:

   ```
   # mkdir ds
   # cd ds
   ```
3. If you have not already done so, download the product binaries file to the installation directory.
4. On UNIX, unpack the product binaries file using the following command:

   ```
   # gunzip -dc filename.tar.gz | tar -xvof -
   ```

where *filename* corresponds to the product binaries you want to unpack.

On a Windows system, unzip the product binaries.

5. Run the `setup` program. You can find it in the directory in which you untarred or unzipped the binary files. On a UNIX system, issue the following command:

   ```
   ./setup
   ```

   Select "yes" to continue with installation, then select "yes" to agree to the license.

6. When you are asked what you would like to install, select the default, Netscape Servers.

7. When you are asked what type of installation you would like to perform, select Express Installation.

8. For server root or destination directory, enter a full path to the location where you want to install your server.

   The location that you enter must be some directory other than the directory from which you are running the setup program. Also, the name of the directory where you install files must not contain any space characters. If the directory that you specify does not exist, the `setup` program creates it for you.

9. UNIX only. For the user and group to run the servers as, enter the identity that you want this server to run as. For more information on the user and groups that you should use when running Netscape servers, see "Deciding the User and Group for Your Netscape Servers (UNIX only)," on page 14.

10. For Configuration Directory Administrator ID and password, enter the name and password that you will log in as when you want to authenticate to the console with full privileges (think of this as the root or superuser identity for the Netscape Console).

The server is then unpackaged, minimally configured, and started. You are told what host and port number on which the is listening.

Note the following about your new Directory Server installation:

- The Directory Server is listening on port 389.
- The server is configured to use the following suffixes:
  - `dc=`*your_machine's_DNS_domain_name*
    That is, if your machine is named `test.example.com`, then you will have the suffix `dc=example,dc=com` configured for this server.

- `o=NetscapeRoot`
  Do not modify the contents of the directory under the `o=NetscapeRoot` suffix. Either create data under the first suffix or create a new suffix to be used for this purpose. For details on how to create new suffixes for your Directory Server, see the *Netscape Directory Server Administrator's Guide*.

Using Typical Installation

Most first time installations of Directory Server can be performed using the Typical Installation option of the `setup` program. Typical installation differs slightly depending on whether you are installing on UNIX or Windows. The following sections outline the different procedures.

Using Typical Installation on UNIX

To perform a typical installation on UNIX:

1. Log in as `root`.
2. Create a new directory:

   ```
   # mkdir ds
   # cd ds
   ```

3. If you have not already done so, download the product binaries file to the installation directory.
4. Unpack the product binaries file using the following command:

   `# gunzip -dc` *`filename`*`.tar.gz | tar -xvof -`

   where *filename* corresponds to the product binaries that you want to unpack.
5. Run the `setup` program. You can find it in the directory where you untarred binary files. Issue the following command from the installation directory:

   `./setup`
6. The `setup` program asks if you would like to proceed with the setup. Press Enter to respond with the default (the default for this prompt is Yes) or press n if you would like to exit the `setup` program.

   If you want to log in as root or superuser (su), you will need to exit the `setup` program.

7. Next, the `setup` program asks you if you agree to the license terms. Press “y” to agree with the license terms.
8. When you are asked what you would like to install, press Enter to select the default, Netscape Servers.
9. When you are asked what type of installation you would like to perform, press Enter to select the default, Typical Installation.
10. For server root, enter a full path to the location where you want to install your server.

    The location that you enter must be some directory other than the directory from which you are running setup. Also, the name of the directory where you install files must not contain any space characters. If the directory that you specify does not exist, setup creates it for you.

    By default, the `setup` program provides the following path:

    `/usr/netscape/servers`

    If you want to install the software into this directory tree, press Enter; otherwise, supply your own path.
11. For the Server Products Core Components, Directory Suite, Administration Services, nsPerl, and PerLDAP, press Enter to select the default (all components).
12. Press Enter to select all of the Server Products Core Components.
13. Press Enter to select all the Directory Suite components.
14. Press Enter to select all of the Administration Services components (Netscape Administration Server and the Administration Server Console).
15. Press Enter to install nsPerl.
16. Press Enter to install PerLDAP.
17. For the hostname, enter a fully qualified hostname or select the default (which is the local host).

CAUTION Note that the default hostname may be incorrect if the installer cannot locate a DNS name in your system. For example, you might not have a DNS name if your system uses NIS.

The hostname must be a fully qualified host and domain name. If the default hostname is not a fully qualified host and domain name, installation will fail. Refer to "Common Installation Problems," on page 119 for more information about entering a fully qualified domain name.

18. The `setup` program then asks you for the System User and the System Group names. Enter the identity under which you want the servers to run.

    For more information on the user and group names that you should use when running Netscape servers, see "Deciding the User and Group for Your Netscape Servers (UNIX only)," on page 14.

19. For the configuration directory, select the default if this directory will host your `o=NetscapeRoot` tree. Otherwise, enter `Yes`. You will then be asked for the contact information for the configuration directory.

    If the server you are currently installing is not the configuration directory, then the configuration directory must exist before you can continue this installation.

20. The `setup` program then asks if the server you are currently installing will be the one for your user data. For most cases, you can select the default. However, if you intend this server instance to be used as a configuration directory only, then you should enter `Yes`.

21. For the Directory Server port, select the default (389) unless you already have another application using that port.

22. For the Directory Server Identifier, enter a unique value (normally the default is sufficient).

    This value is used as part of the name of the directory in which the Directory Server instance is installed. For example, if your machine's host name is `phonebook`, then this name is the default and selecting it will cause the Directory Server instance to be installed into a directory labeled `slapd-phonebook`.

CAUTION The Directory Server identifier must not contain a period. For example, `example.server.com` is not a valid server identifier name.

23. For Configuration Directory Administrator ID and password, enter the name and password that you will log in as when you want to authenticate to the console with full privileges.

24. For a directory suffix, enter a distinguished name (DN) meaningful to your enterprise.

    This string is used to form the name of all your organization's directory entries. Therefore, pick a name that is representative of your organization. It is recommended that you pick a suffix that corresponds to your internet DNS name. Avoid space characters in the suffix.

    For example, if your organization uses the DNS name `example.com`, then enter `dc=example,dc=com` here.

25. For Directory Manager DN, enter the DN that you will use when managing the contents of your directory with unlimited privileges.

NOTE Any DN must be entered in the UTF-8 character set encoding. Older encodings such as ISO-8859-1 are not supported.

    In former releases of Directory Server, the Directory Manager was known as the root DN. This is the entry that you bind to the directory as when you want access control to be ignored. This DN can be short and does not have to conform to any suffix configured for your directory. However, it should not correspond to an actual entry stored in your directory.

26. For the Directory Manager password, enter a value that is at least 8 characters long.

27. For Administration Domain, enter the domain that you want this server to belong to.

    The name you enter should be a unique string that is descriptive of the organization responsible for administering the domain. For information on administration domains, see "Determining the Administration Domain," on page 18.

28. For the administration port number, enter a value that is not in use. Be sure to record this value.

29. For the user you want to run Administration Server as, enter `root`. This is the default.

    For information on why you should run Administration Server as root, see "Deciding the User and Group for Your Netscape Servers (UNIX only)," on page 14.

The server is then unpackaged, minimally configured, and started. You are told what host and port number Administration Server is listening on.

The server is configured to use the following suffixes:

- The suffix that you configured.
- `o=NetscapeRoot`

Do not modify the contents of the directory under the `o=NetscapeRoot` suffix. Either create data under the first suffix or create a new suffix to be used for this purpose. For details on how to create new suffixes for your Directory Server, see the *Netscape Directory Server Administrator's Guide*.

Using Typical Installation on Windows

To perform a typical installation on Windows:

1. Log in as a user with administrator privileges.
2. If you have not already done so, download the product binaries file to the installation directory.
3. Unzip the product binaries files and run the `setup` program.
4. When you are asked what you would like to install, select the default, Netscape Servers.
5. When you are asked what type of installation you would like to perform, select the default, Typical.
6. For server installation root, enter a full path to the location where you want to install your server.

   The location that you enter must be some directory other than the directory from which you are running setup. If the directory that you specify does not exist, the `setup` program creates it for you.

7. For configuration directory, select the default if this directory will host your `o=NetscapeRoot` tree. Otherwise, enter the appropriate contact information for the configuration directory.

   If this Directory Server instance is not the configuration directory, then the configuration directory must exist and be running before you can continue this installation.

8. For the directory to store data in, you must decide if this Directory Server instance will store your enterprise's data. For most cases, you can select the default, "Store data in this Directory Server." However, if this Directory Server instance is intended to be a configuration directory only, then you should select "Store data in an existing Directory Server."

9. For server identifier, enter a unique value (normally the default is sufficient).

   This value is used as part of the name of the directory in which the Directory Server instance is installed. For example, if your machine's host name is `phonebook` then this name is the default and selecting it will cause the Directory Server instance to be installed into a directory labeled `slapd-phonebook`.

10. For a directory suffix, enter a distinguished name (DN) that is meaningful to your enterprise.

    This string is used to form the name of all your organization's directory entries. Therefore, pick some name that is representative of your organization. It is recommended that you pick a suffix that corresponds to your Internet DNS name. For example, if your organization uses the DNS name `example.com`, then enter `dc=example,dc=com` here. Avoid space characters in the suffix.

11. For the Directory Server port, select the default (389) unless you already have another application using that port.

12. For Configuration Directory Administrator ID and password, enter the name and password that you will log in as when you want to authenticate to the console with full privileges.

13. For Administration Domain, enter the domain to which you want this server to belong.

    The name that you enter should be a unique string that is descriptive of the organization responsible for administering the domain. For information on administration domains, see "Determining the Administration Domain," on page 18.

14. For Directory Manager DN, enter the DN that you will use when managing the contents of your directory with unlimited privileges.

NOTE Any DN must be entered in the UTF-8 character set encoding. Older encodings such as ISO-8859-1 are not supported.

In former releases of Directory Server, the Directory Manager was known as the root DN. This is the entry that you bind to the directory as when you want access control to be ignored. This DN can be short and does not have to conform to any suffix configured for your directory. However, it should not correspond to an actual entry stored in your directory.

15. For Directory Manager password, enter a value that is at least 8 characters long.
16. For administration port number, enter a value that is not in use. Be sure to record this value.

The server is then unpackaged, minimally configured, and started. You are told which host and port number the Administration Server is listening on.

The server is configured to use the following suffixes:

- The suffix that you configured.
- `o=NetscapeRoot`

Do not modify the contents of the directory under the `o=NetscapeRoot` suffix. Either create data under the first suffix or create a new suffix to be used for this purpose. For details on how to create new suffixes for your Directory Server, see the *Netscape Directory Server Administrator's Guide*.

Chapter 3

Computer System Requirements

Before you can install Netscape Directory Server (Directory Server), you must make sure that the systems on which you plan to install the software meet the minimum hardware and operating system requirements.

These requirements are described in detail for each platform in the following sections:

- Summary of Supported Platforms (page 33)
- Hardware Requirements (page 36)
- Operating System Requirements (page 36)

Summary of Supported Platforms

This release of Directory Server is supported on the platforms listed in Table 3-1. The sections that follow provide information that is specific to each of the supported platforms.

Before you install Directory Server, check the required patches and kernel parameter settings, as described in the sections that follow. Also ensure that DNS is properly configured on the system and that the system has a static IP address.

Table 3-1 Supported Platforms

HP-UX® Platform Requirements	
OS Version	HP UX 11.0 or HP UX 11i with relevant patches. For details, see “HP-UX 11.0 or 11i Operating System” on page 37.
CPU	HP 9000 architecture with a PA-RISC 1.1 or PA-RISC 2.0 CPU.

Table 3-1 Supported Platforms *(Continued)*

Memory / RAM	256 MB. However, you should plan from 512 MB to 1 GB of RAM for best performance on large production systems.
Storage Space / Hard Disk	Approximately 300 MB of disk space for a minimal installation. For production systems, you should plan at least 2 GB to support the product binaries, databases, and log files (log files require 1 GB by default); 4GB and greater may be required for very large directories.
Other Requirements	You must install as root in order to use well-known port numbers (such as 389) that are less than 1024. If you do not plan to use port numbers less than 1024, you do not need to install as root. If you plan to run as root, you should also install as root and specify nobody, or a similar user ID that has very few privileges, as the default run-as user and group.
Microsoft Windows® Platform Requirements	
OS Version	Windows 2000 Advanced Server with Service Pack 3. For details, see “Microsoft Windows 2000 Advanced Server” on page 41.
CPU	350 MHz or higher, Pentium 4 compatible.
Memory / RAM	256 MB. However, you should plan from 256 MB to 1 GB of RAM for best performance on large production systems.
Storage Space / Hard Disk	Approximately 300 MB of disk space for a minimal installation. For production systems, you should plan at least 2 GB to support the product binaries, databases, and log files (log files require 1 GB by default); 4GB and greater may be required for very large directories. To support database files that are larger than 2 GB, the machine must be configured to support large files; you can do this by choosing `vxfs` filesystem with `largefiles` option.
Other Requirements	You must install as Administrator or a user with Administrator privileges (that is, the user must be in the Administrators group). For additional details, see “Microsoft Windows 2000 Advanced Server” on page 41.
Red Hat Linux® Platform Requirements	
OS Version	Linux 7.3 (x86) or Linux Advanced Server 2.1 (x86) with relevant upgrades / patches. For details, see “Red Hat Linux 7.3 Operating System” on page 44 or “Red Hat Linux Advanced Server 2.1 Operating System” on page 50.
CPU	350 MHz or higher, Pentium 4 compatible.
Memory / RAM	256 MB. However, you should plan from 256 MB to 1 GB of RAM for best performance on large production systems.

Table 3-1 Supported Platforms *(Continued)*

Storage Space / Hard Disk	Approximately 300 MB of disk space for a minimal installation. For production systems, you should plan at least 2 GB to support the product binaries, databases, and log files (log files require 1 GB by default); 4GB and greater may be required for very large directories.
Other Requirements	You must install as root in order to use well-known port numbers (such as 389) that are less than 1024. If you do not plan to use port numbers less than 1024, you do not need to install as root. If you plan to run as root, you should also install as root and specify nobody as the default run-as user and group.
Sun Solaris® Platform Requirements	
OS Version	Solaris 8 (32-bit) or Solaris 9 (32-bit) with relevant patches. For details, see “Sun Solaris 8 Operating System” on page 54 or “Sun Solaris 9 Operating System” on page 61. Solaris bits can run in 32-bit or 64-bit operating system mode (32 bit application certified on 64 bit mode).
CPU	Ultra 10 or faster (32 bit).
Memory / RAM	256 MB. However, you should plan from 512 MB to 1 GB of RAM for best performance on large production systems.
Storage Space / Hard Disk	Approximately 300 MB of disk space for a minimal installation. For production systems, you should plan at least 2 GB to support the product binaries, databases, and log files (log files require 1 GB by default); 4GB and greater may be required for very large directories. To support database files that are larger than 2 GB, the machine must be configured to support large files; you can do this by choosing `largefile`.
Other Requirements	You must install as `root` in order to use well-known port numbers (such as 389) that are less than 1024. If you do not plan to use port numbers less than 1024, you do not need to install as `root`. If you plan to run as `root`, you should also install as `root` and specify nobody, or a similar user ID that has very few privileges, as the default run-as user and group.

Hardware Requirements

On all platforms, you will need:

- Roughly 200 MB of disk space for a minimal installation. For production systems, you should plan at least 2GB to support the product binaries, databases, and log files (log files require 1 GB by default); 4GB and greater may be required for very large directories.
- 256 MB of RAM. However, you should plan from 256 MB to 1 GB of RAM for best performance on large production systems.

The table below contains some guidelines for disk space and memory requirements depending on the number of entries managed by your Directory Server. This assumes entries in the LDIF file are approximately 100 bytes in size and only the recommended indexes are configured. If you are using larger entries, make sure that at least four times the size of the LDIF file is available on disk.

Number of Entries	Disk Space and Memory Required
10,000 - 250,000 entries	Free disk space: 2 GB Free memory: 256 MB
250,000 - 1,000,000 entries	Free disk space: 4 GB Free memory: 512 MB
Over 1,000,000 entries	Free disk space: 8GB Free memory: 1 GB

Operating System Requirements

This section contains information on operating-system versions and patches required for installing Directory Server:

- dsktune Utility
- HP-UX 11.0 or 11i Operating System
- Microsoft Windows 2000 Advanced Server
- Red Hat Linux 7.3 Operating System
- Red Hat Linux Advanced Server 2.1 Operating System
- Sun Solaris 8 Operating System
- Sun Solaris 9 Operating System
- DNS and NIS Requirements (UNIX Only)

dsktune Utility

For UNIX platforms, Directory Server provides a utility named `dsktune` that can help you verify whether you have the appropriate patches installed on your system. The utility also provides useful information and advice on how to tune your kernel parameters for best performance.

To enable you to run `dsktune` before installing the Directory Server, the utility is placed, along with the `setup` program, in the directory where you unpack product binaries. Additionally, in the 6.2 release, the `setup` program has been enhanced to allow specifying of a pre-pre-installation program to be run before the Directory Server installation begins—in the `slapd.inf` file, a new field named `PrePreInstall` is defined for specifying the path to the executable, which must be relative to the `setup` program. By default, the `PrePreInstall` field is set to the `dsktune` utility path, enabling you to run the utility as a part of the Directory Server installation.

After you've installed the Directory Server, you can find the utility in this directory:

serverRoot`/bin/slapd/server`

For information on running `dsktune`, see Chapter 8, "Troubleshooting."

HP-UX 11.0 or 11i Operating System

This section contains the following information:

- Verifying Disk Space Requirements
- Verifying Required System Modules
- Installing Patches
- Tuning the System
- Installing Third-Party Utilities

Verifying Disk Space Requirements

Ensure that you have sufficient disk space before downloading the software.

Download drive: 120 MB
Installation drive: 2 GB

Verifying Required System Modules

Directory Server is not supported on HP-UX 10 or earlier versions. The minimum system module required is HP-UX 11. Directory Server may be used on a 64 bit HP-UX 11 environment, but will run as a 32 bit process, and is limited to 1 GB of process memory.

For best results, Directory Server requires an HP 9000 architecture with a PA-RISC 1.1 or PA-RISC 2.0 CPU.

Installing Patches

Before you install Directory Server, ensure that the host system is updated with the latest patches recommended by the operating-system vendor. Because the list of recommended patches changes with time, you must always check the operating system vendor's site for a list of patches that you may need to install. Listed below are two URLs to aid you in this effort:

`http://welcome.hp.com/country/us/eng/support.htm`
`http://www.hp.com/products1/unix/java/`

Here are some recommendations:

- For HP-UX 11.0, install the latest `HP-UX 11.0 Quality Pack (QPK1100)` patch. For HP-UX 11i, install the latest `HP-UX 11i Quality Pack (GOLDQPK11i)` patch. For details, see `http://www.software.hp.com/SUPPORT_PLUS/qpk.html`.
- Install the patches listed below.

PHKL_18543:	PM / VM / UFS / async / scsi / io / DMAPI / JFS / perf cumulative patch
PHCO_23651:	fsck_vxfs(1M) cumulative patch
PHCO_19666:	libpthread cumulative patch
PHKL_20228:	Large data 7 / 8 patch
PHKL_21039:	semget;large data space;msgmnb;SEMMSL
PHKL_23409:	NFS, Large Data Space, kernel memory leak patch
PHCO_16629:	libc cumulative patch (superceded by PHCO_20765)
PHCO_20765:	libc cumulative patch (supercedes PHCO_16629 and is superceded by PHCO_24148)
PHCO_24148:	libc cumulative patch (supercedes PHCO_20765)
PHKL_17709:	libpthread cumulative patch (superceded by PHKL_17935)

PHSS_16587:	HP aC++ runtime libraries
PHKL_20335:	boot,Jfs;IO perf;PA8600;3GB data;NFS;bcache
PHKL_20174:	Allow sam to set maxdsize patch
PHCO_21187:	Cumulative SAM/ObAM patch

- Install the patches listed below; Netscape Console uses the Abstract Window Tool (AWT) kit and requires you to install these patches.

PHSS_25290:	Xserver cumulative patch
PHSS_25091:	Font Server JAN 99 Cumulative Patch
PHSS_25199:	CDE Runtime JUNE2001 Periodic Patch
PHSS_25447:	X/Motif 32bit Runtime APR2001 Periodic Patch
PHSS_25879:	X/Motif 64bit Runtime JUL2001 Periodic Patch
PHSS_25766:	Asian Printer cumulative patch The following patches are dependencies of patch PHSS_25766: PHCO_18230 and PHSS_20192.
PHSS_20189:	ASX release notes NOV 1999 cumulative patch
PHSS_20190:	Asian Input Method NOV 1999 cumulative patch
PHNE_26771:	Cumulative ARPA Transport patch The following patches are dependencies of patch PHNE_26771: PHKL_21857 and PHNE_22566.

- Run the `dsktune` utility and see if you need to install any other patches. The utility helps you to verify whether you have the appropriate patches installed on your system and provides useful information and advice on how to tune your kernel parameters for best performance. For information on the `dsktune` utility, see “dsktune Utility” on page 37.”

Tuning the System

Set your kernel parameters as follows:

- Set `maxfiles` to 100 (the old value was 60).
- Set `nkthread` to 1328 (the old value was 499); `nkthread` is a computed value: `(((NPROC*7)/4+16)`.

- Set max_thread_proc to 512 (the old value was 64).
- Set maxusers to 64 (the old value was 32).
- Set maxuprc to 512 (the old value was 75).
- Set nproc to 750, a new value which is not based on a formula (the old formula was 20+8*MAXUSERS, which evaluated to 276).

Typically, client applications that do not properly shut down the socket cause it to linger in a TIME_WAIT state. To prevent this, you should consider changing the TIME_WAIT setting to a reasonable value. For example, setting

```
ndd -set /dev/tcp tcp_time_wait_interval 60000
```

will limit the TIME_WAIT state of sockets to 60 seconds.

You also need to turn on large file support in order for Directory Server to work properly. To change an existing file system (from one that has no large files to one that accepts large files):

1. Unmount the system using the umount command. For example:

   ```
   umount /export
   ```

2. Create the large file system. For example:

   ```
   fsadm -F vxfs -o largefiles /dev/vg01/rexport
   ```

3. Remount the file system. For example:

   ```
   /usr/sbin/mount -F vxfs -o largefiles /dev/vg01/export
   ```

For additional information and recommendations about setting these parameters, consult your operating-system documentation.

Installing Third-Party Utilities

You will need the gunzip utility to unpack the Directory Server software. The GNU gzip and gunzip programs are described in more detail at http://www.gnu.org/software/gzip/gzip.html and can be obtained from many software distribution sites.

You may need Adobe Acrobat Reader to read the documentation. If you do not have it installed, you can download it from:

http://www.adobe.com/products/acrobat/readstep2.html

Microsoft Windows 2000 Advanced Server

If you plan to install Directory Server on a machine running the Windows 2000 Advanced Server operating system (OS), follow the recommendations outlined in these sections:

- Configuring a Machine to Run Directory Server
- Verifying Required System Modules
- Installing Windows 2000 Server
- Installing Third-Party Utilities
- Ensuring System Clock Accuracy
- Installing Windows Service Packs and Hotfixes
- Configuring the System Post Installation

In addition to these recommendations, be sure to check the OS vendor's web site for the latest information pertaining to your OS version. Below are two URLs that you may find useful:

`http://www.microsoft.com/technet/`

`http://support.microsoft.com/`

Configuring a Machine to Run Directory Server

Directory Server must be installed with a static IP address on a computer that is isolated from the public Internet by a network-level firewall. This is necessary to protect the operating system from IP-based attacks.

No other network functions should be provided by this computer. The computer should not be a dual-booting system or run other operating systems. At a minimum, the computer system should have at least 256 MB of RAM, 2 GB of disk, a Pentium 4 or later processor, and a 100 MBps Ethernet connection.

Ensure that you have sufficient disk space before downloading the software.

Download drive: 120 MB
Installation drive: 200 MB

Verifying Required System Modules

Directory Server is not supported on *Windows 2000 Pro* or *Windows 2000 DataCenter Server*.

Installing Windows 2000 Server

During the installation of Windows 2000, observe the following:

- If there is already an operating system present on the computer, choose to perform a fresh install rather than an upgrade.
- Format the drives with NTFS rather than FAT, as NTFS allows access controls to be set on files and directories.
- Specify that the computer will be a standalone server and will not be a member of any existing domain or workgroup. This will reduce dependencies on the network security services.
- Choose an administrator password of at least 9 characters. Use punctuation or other non-alphabetic characters in the first 7 characters.
- Do not install Internet Information Server.
- Specify only TCP/IP as network protocol, and do not install any other network services.

Installing Third-Party Utilities

You need an UNZIP utility to unpack the directory server software. There are many commercially licensed, free and shareware tools available, such as PKZIP or Winzip. Note that shareware unregistered versions of PKZIP 2.70 maintain a TCP/IP connection to an Internet advertising service, so it may not be suitable for installation on this system.

You may need Adobe Acrobat Reader to read the documentation. If you do not have it installed, you can download it from:
`http://www.adobe.com/products/acrobat/readstep2.html`

To edit the server configuration file, you will need a text editor that is capable of handling large text files (Notepad and Wordpad are not suitable). If you are already familiar with Emacs text editor on UNIX, a port to Windows can be downloaded from `ftp://ftp.cs.washington.edu/pub/ntemacs/`. There are many other shareware and commercial text editors available.

To display non-English characters using any Netscape browser, you can obtain general internationalization advice and more specific information about the Bitstream Cyberbit font from the following URL:

`http://developer.netscape.com/software/jdk/i18n.html`

To download the Bitstream Cyberbit font use the following FTP link:

`ftp://ftp.netscape.com/pub/communicator/extras/fonts/windows`

Before downloading the font, read the `READMEfirst.txt` and `ReadMe.htm` files.

Ensuring System Clock Accuracy

To facilitate the correlation of date and time stamps in log files with those of other computer systems, keep your system clock reasonably in sync. As the NET TIME command requires NetBIOS, which will be disabled during post-installation system configuration, either a TCP/IP based NTP client should be installed (such as the shareware program Tardis), or a time radio receiver attached. See `http://www.ntp.org` for more information on NTP clients for Windows.

Installing Windows Service Packs and Hotfixes

Windows 2000 Service Packs include key fixes that are needed to maintain the security and reliability of the operating system. The hotfix series contains important changes for problems discovered after the service pack had been released.

Directory Server is certified with Service Pack 3 and security patches released by the OS vendor at the time of this certification. It is recommended that you install the latest service pack and all hotfixes and patches recommended by the OS vendor.

Configuring the System Post Installation

The Windows 2000 environment requires tuning to provide optimum performance for Directory Server in an operational environment. Consult the Windows 2000 system administrator's documentation or support channel for information on Windows 2000 tuning for multi-threaded internet services.

It is recommended that you set the `LargeSystemCache` registry key to 0 to limit the growth of system cache. The `LargeSystemCache` has a default value of 1, which is not suitable for applications such as Directory Server, which do caching internally.

Also, if there'll be a lot of connections from clients:

- Change `tcp_time_wait_interval` from its default value, which is 240 seconds, to 60 seconds. To do this, at Registry `HKEY_LOCAL_MACHINE\System\CurrectControlSet\services\Tcpip\Parameters`, create a key `TcpTimeWaitDelay` with value 60.

- Change the upper range of ephemeral from the default value, which is 4999, to 65534. To do this, at Registry `HKEY_LOCAL_MACHINE\System\CurrectControlSet\services\Tcpip\Parameters`, create a key `MaxUserPort` with value 65534.

Red Hat Linux 7.3 Operating System

If you plan to install Directory Server on a machine running the Linux 7.3 operating system (OS), follow the recommendations outlined in these sections:

- Verifying Disk Space Requirements
- Verifying Required System Modules
- Installing System Patches
- Tuning the System
- Installing Third-Party Utilities

In addition to these recommendations, be sure to check the OS vendor's web site for the latest information pertaining to your OS version:

`http://www.redhat.com/apps/support/`

Verifying Disk Space Requirements

Ensure that you have sufficient disk space before downloading the software.

Download drive: 120 MB
Installation drive: 2 GB

Verifying Required System Modules

Directory Server is certified to work on:

- The Intel Pentium series processors [i686]
- The default kernel / glibc revisions that comes along with Red Hat Linux 7.3 and the other kernel revisions with their corresponding glibc revisions as mentioned below.
    - Required Kernel:

      Default kernel - kernel-2.4.18-3
      Kernel used for certification - 2.4.18-27.7
    - Required glibC:

Default glibc - glibc-2.2.5-34
glibc used for certification - glibc-2.2.5-43

- Required Filesytem:

  ext3 (`LARGEFILES` support enabled) filesystem has been used for the certification process.

Installing System Patches

Directory Server has been certified on Red Hat Linux 7.3 with kernel revisions 2.4.18-27.7.x (`kernel-2.4.18-27.7.x.i686.rpm`) / glibc version 2.2.5-43 (`glibc-2.2.5-43.i686.rpm`). Table 3-2 provides the list of `.rpm` packages that were installed in the test machines during the certification process of this release of Directory Server. (If the machine is a single CPU machine, the corresponding kernel would be of the form `kernel-x.x.x.x`. If the machine is a multi-CPU machine, then the corresponding kernel would be of the form `kernel-smp-x.x.x.x`.)

Table 3-2 Red Hat Linux 7.3 Patch List

ark-3.0.3-0.7.i386.rpm	ksirc-3.0.3-0.7.2.i386.rpm
arts-1.0.3-0.7.1.i386.rpm	ktalkd-3.0.3-0.7.2.i386.rpm
arts-devel-1.0.3-0.7.1.i386.rpm	ktimer-3.0.3-0.7.i386.rpm
balsa-1.2.4-7.7.3.i386.rpm	kview-3.0.3-0.7.2.i386.rpm
bind-utils-9.2.1-1.7x.2.i386.rpm	kviewshell-3.0.3-0.7.2.i386.rpm
Canna-3.5b2-62.7.3.i386.rpm	kviewshell-devel-3.0.3-0.7.2.i386.rpm
Canna-libs-3.5b2-62.7.3.i386.rpm	kxmlrpcd-3.0.3-0.7.2.i386.rpm
cervisia-3.0.3-0.7.i386.rpm	libesmtp-0.8.12-0.7.x.i386.rpm
compat-libstdc++-6.2.rpm	libesmtp-devel-0.8.12-0.7.x.i386.rpm
cpp-2.96-113.i386.rpm	libgal19-0.19.2-3.7x.i386.rpm
cups-1.1.14-15.2.i386.rpm	libkscan-3.0.3-0.7.2.i386.rpm
cups-devel-1.1.14-15.2.i386.rpm	libkscan-devel-3.0.3-0.7.2.i386.rpm
cups-libs-1.1.14-15.2.i386.rpm	libpng-1.0.14-0.7x.4.i386.rpm
cvs-1.11.1p1-8.7.i386.rpm	libpng-devel-1.0.14-0.7x.4.i386.rpm
dateconfig-0.7.5-7.i386.rpm	libstdc++-2.96-113.i386.rpm
evolution-1.0.8-9.7x.1.i386.rpm	libstdc++-devel-2.96-113.i386.rpm
fetchmail-5.9.0-21.7.3.i386.rpm	lisa-3.0.3-0.7.2.i386.rpm

Table 3-2 Red Hat Linux 7.3 Patch List *(Continued)*

file-3.39-8.7x.i386.rpm	losetup-2.11n-12.7.3.i386.rpm
fileutils-4.1-10.1.i386.rpm	LPRng-3.8.9-4.i386.rpm
gaim-0.59.1-0.7.3.i386.rpm	mew-2.2-5.7x.i386.rpm
gal-0.19.2-3.7x.i386.rpm	mew-common-2.2-5.7x.i386.rpm
gal-devel-0.19.2-3.7x.i386.rpm	mm-1.1.3-11.i386.rpm
galeon-1.2.6-0.7.3.i386.rpm	mm-devel-1.1.3-11.i386.rpm
gcc-2.96-113.i386.rpm	modutils-2.4.18-3.7x.i386.rpm
gcc-c++-2.96-113.i386.rpm	mount-2.11n-12.7.3.i386.rpm
gcc-g77-2.96-113.i386.rpm	mozilla-1.0.1-2.7.3.i386.rpm
gcc-objc-2.96-113.i386.rpm	mozilla-chat-1.0.1-2.7.3.i386.rpm
gdb-5.2-2.i386.rpm	mozilla-devel-1.0.1-2.7.3.i386.rpm
ghostscript-6.52-9.4.i386.rpm	mozilla-dom-inspector-1.0.1-2.7.3.i386.rpm
glibc-2.2.5-43.i686.rpm	mozilla-js-debugger-1.0.1-2.7.3.i386.rpm
glibc-common-2.2.5-43.i386.rpm	mozilla-mail-1.0.1-2.7.3.i386.rpm
glibc-devel-2.2.5-43.i386.rpm	mozilla-nspr-1.0.1-2.7.3.i386.rpm
glibc-kernheaders-2.4-7.16.i386.rpm	mozilla-nspr-devel-1.0.1-2.7.3.i386.rpm
hwdata-0.14.1-1.noarch.rpm	mozilla-nss-1.0.1-2.7.3.i386.rpm
kaboodle-3.0.3-0.7.1.i386.rpm	mozilla-nss-devel-1.0.1-2.7.3.i386.rpm
karm-3.0.3-0.7.i386.rpm	mozilla-psm-1.0.1-2.7.3.i386.rpm
kcalc-3.0.3-0.7.i386.rpm	nautilus-1.0.6-16.i386.rpm
kcharselect-3.0.3-0.7.i386.rpm	nautilus-devel-1.0.6-16.i386.rpm
kde-i18n-Japanese-3.0.3-0.7.3.noarch.rpm	nautilus-mozilla-1.0.6-16.i386.rpm
kdeaddons-kate-3.0.3-0.7.i386.rpm	netpbm-9.24-9.73.2.i386.rpm
kdeaddons-kicker-3.0.3-0.7.i386.rpm	netpbm-devel-9.24-9.73.2.i386.rpm
kdeaddons-knewsticker-3.0.3-0.7.i386.rpm	netpbm-progs-9.24-9.73.2.i386.rpm
kdeaddons-konqueror-3.0.3-0.7.i386.rpm	noatun-3.0.3-0.7.1.i386.rpm
kdeaddons-noatun-3.0.3-0.7.i386.rpm	nscd-2.2.5-43.i386.rpm
kdeadmin-3.0.3-0.7.i386.rpm	nss_ldap-189-4.i386.rpm
kdeartwork-3.0.3-0.7.1.i386.rpm	openldap-2.0.27-2.7.3.i386.rpm
kdeartwork-locolor-3.0.3-0.7.1.i386.rpm	openldap-clients-2.0.27-2.7.3.i386.rpm

Table 3-2 Red Hat Linux 7.3 Patch List *(Continued)*

kdeartwork-screensavers-3.0.3-0.7.1.i386.rpm
kdebase-3.0.3-0.7.2.i386.rpm
kdebase-devel-3.0.3-0.7.2.i386.rpm
kdegames-3.0.3-0.7.i386.rpm
kdegames-devel-3.0.3-0.7.i386.rpm
kdelibs-3.0.3-0.7.2.i386.rpm
kdelibs-devel-3.0.3-0.7.2.i386.rpm
kdemultimedia-arts-3.0.3-0.7.1.i386.rpm
kdemultimedia-devel-3.0.3-0.7.1.i386.rpm
kdemultimedia-kfile-3.0.3-0.7.1.i386.rpm
kdemultimedia-libs-3.0.3-0.7.1.i386.rpm
kdenetwork-devel-3.0.3-0.7.2.i386.rpm
kdenetwork-libs-3.0.3-0.7.2.i386.rpm
kdepasswd-3.0.3-0.7.i386.rpm
kdepim-3.0.3-0.7.i386.rpm
kdepim-cellphone-3.0.3-0.7.i386.rpm
kdepim-devel-3.0.3-0.7.i386.rpm
kdepim-pilot-3.0.3-0.7.i386.rpm
kdesdk-kapptemplate-3.0.3-0.7.i386.rpm
kdesdk-kbabel-3.0.3-0.7.i386.rpm
kdesdk-kbugbuster-3.0.3-0.7.i386.rpm
kdesdk-kmtrace-3.0.3-0.7.i386.rpm
kdesdk-kompare-3.0.3-0.7.i386.rpm
kdesdk-kspy-3.0.3-0.7.i386.rpm
kdessh-3.0.3-0.7.i386.rpm
kdevelop-2.1.3-0.7.1.i386.rpm
kdf-3.0.3-0.7.i386.rpm
kdict-3.0.3-0.7.2.i386.rpm
kedit-3.0.3-0.7.i386.rpm
kernel-2.4.18-27.7.x.i686.rpm
openldap-devel-2.0.27-2.7.3.i386.rpm
openssh-3.1p1-6.i386.rpm
openssh-askpass-3.1p1-6.i386.rpm
openssh-askpass-gnome-3.1p1-6.i386.rpm
openssh-clients-3.1p1-6.i386.rpm
openssh-server-3.1p1-6.i386.rpm
openssl-0.9.6b-30.7.i686.rpm
openssl-0.9.6b-32.7.i686.rpm
openssl-devel-0.9.6b-30.7.i386.rpm
openssl-devel-0.9.6b-32.7.i386.rpm
pam-0.75-46.7.3.i386.rpm
pam-devel-0.75-46.7.3.i386.rpm
perl-Digest-MD5-2.20-1.i386.rpm
pine-4.44-7.73.0.i386.rpm
psmisc-20.2-3.73.i386.rpm
python-1.5.2-43.73.i386.rpm
python-devel-1.5.2-43.73.i386.rpm
python2-2.2.2-11.7.3.i386.rpm
python2-devel-2.2.2-11.7.3.i386.rpm
qt-3.0.5-7.14.i386.rpm
qt-designer-3.0.5-7.14.i386.rpm
qt-devel-3.0.5-7.14.i386.rpm
rhn_register-2.8.27-1.7.3.i386.rpm
rhn_register-gnome-2.8.27-1.7.3.i386.rpm
sane-backends-1.0.7-6.1.i386.rpm
sane-backends-devel-1.0.7-6.1.i386.rpm
scrollkeeper-0.3.4-5.i386.rpm
sendmail-8.11.6-23.73.i386.rpm
sendmail-8.11.6-25.73.i386.rpm
sendmail-cf-8.11.6-23.73.i386.rpm

Table 3-2 Red Hat Linux 7.3 Patch List *(Continued)*

kernel-smp-2.4.18-27.7.x.i686.rpm	sendmail-cf-8.11.6-25.73.i386.rpm
kfloppy-3.0.3-0.7.i386.rpm	sendmail-devel-8.11.6-23.73.i386.rpm
khexedit-3.0.3-0.7.i386.rpm	sendmail-devel-8.11.6-25.73.i386.rpm
kit-3.0.3-0.7.2.i386.rpm	shadow-utils-20000902-9.7.i386.rpm
kjots-3.0.3-0.7.i386.rpm	tar-1.13.25-4.7.1.i386.rpm
kljettool-3.0.3-0.7.i386.rpm	tetex-1.0.7-47.1.i386.rpm
klpq-3.0.3-0.7.i386.rpm	tkinter-1.5.2-43.73.i386.rpm
klprfax-3.0.3-0.7.i386.rpm	ucd-snmp-4.2.5-7.73.0.i386.rpm
kmail-3.0.3-0.7.2.i386.rpm	ucd-snmp-utils-4.2.5-7.73.0.i386.rpm
kmid-3.0.3-0.7.1.i386.rpm	up2date-2.8.39-1.7.3.i386.rpm
kmidi-3.0.3-0.7.1.i386.rpm	up2date-gnome-2.8.39-1.7.3.i386.rpm
kmix-3.0.3-0.7.1.i386.rpm	util-linux-2.11n-12.7.3.i386.rpm
knewsticker-3.0.3-0.7.2.i386.rpm	vim-common-6.1-18.7x.2.i386.rpm
knode-3.0.3-0.7.2.i386.rpm	vim-enhanced-6.1-18.7x.2.i386.rpm
knotes-3.0.3-0.7.i386.rpm	vim-minimal-6.1-18.7x.2.i386.rpm
koncd-3.0.3-0.7.1.i386.rpm	vnc-3.3.3r2-28.2.i386.rpm
korn-3.0.3-0.7.2.i386.rpm	vnc-server-3.3.3r2-28.2.i386.rpm
kpf-3.0.3-0.7.2.i386.rpm	w3m-0.3.1-4.7x.1.i386.rpm
kppp-3.0.3-0.7.2.i386.rpm	wget-1.8.2-4.73.i386.rpm
krb5-devel-1.2.4-11.i386.rpm	xchat-1.8.9-1.73.0.i386.rpm
krb5-libs-1.2.4-11.i386.rpm	xinetd-2.3.7-4.7x.i386.rpm
kregexpeditor-3.0.3-0.7.i386.rpm	xpdf-1.00-5.i386.rpm
kregexpeditor-devel-3.0.3-0.7.i386.rpm	ypserv-2.5-2.7x.i386.rpm
kscd-3.0.3-0.7.1.i386.rpm	-

Tuning the System

This section contains some basic system tuning information. Keep in mind that changing any of the following kernel tuning parameters requires a system reboot.

- NFS Tuning—This tuning is recommended if you are using Directory Server to write to NFS mounted drives. On Linux, NFS is typically recommended to be done over TCP and not over UDP. Make the following change to the `/etc/rc.d/init.d/autofs` file:

  ```
  + localoptions='rsize=8192,wsize=8192,vers=3,tcp'
  ```

- TCP Tuning—You can increase number of local system ports available by running this command:

  ```
  echo "1024 65000" > /proc/sys/net/ipv4.ip_local_port_range
  ```

  You can also achieve the same by editing this parameter in the `/etc/sysctl.conf` file:

  ```
  [ echo "1024 65000" >> /etc/sysctl.conf ]
  ```

- File Tuning—You can increase the file descriptors by running these commands:

  `echo "64000" > /proc/sys/fs/file-max` or edit this parameter in the `/etc/sysctl.conf` file: `[ echo "fs.file-max = 64000" >> /etc/sysctl.conf ]`

  ```
  echo "* soft nofile 8192" >> /etc/security/limits.conf
  ```

  ```
  echo "* hard nofile 8192" >> /etc/security/limits.conf
  ```

  ```
  echo "ulimit -n 8192" >> /etc/profile
  ```

  ```
  echo "session required /lib/security/pam_limits.so" >>
  /etc/security/limits.conf
  ```

Installing Third-Party Utilities

You will need the `gunzip` utility to unpack the Directory Server software. The GNU `gzip` and `gunzip` programs are described in more detail at `http://www.gnu.org/software/gzip/gzip.html` and can be obtained from many software distribution sites.

You may need Adobe Acrobat Reader to read the documentation. If you do not have it installed, you can download it from: `http://www.adobe.com/products/acrobat/readstep2.html`

Red Hat Linux Advanced Server 2.1 Operating System

If you plan to install Directory Server on a machine running the Linux Advanced Server 2.1 operating system (OS), follow the recommendations outlined in these sections:

- Verifying Disk Space Requirements
- Verifying Required System Modules
- Installing System Patches
- Tuning the System
- Installing Third-Party Utilities

In addition to these recommendations, be sure to check the OS vendor's web site for the latest information pertaining to your OS version:

`http://www.redhat.com/apps/support/`

Verifying Disk Space Requirements

Ensure that you have sufficient disk space before downloading the software.

Download drive: 120 MB
Installation drive: 2 GB

Verifying Required System Modules

Directory Server is certified to work on:

- The Intel Pentium series processors [i686]
- The default kernel/glibc revisions that comes along with Red Hat Linux Advanced Server 2.1 and the other kernel revisions with their corresponding glibc revisions as mentioned below.
    - Required Kernel:

      Default kernel - kernel-2.4.9-e.3
      Kernel used for certification - kernel-2.4.9-e.16
    - Required glibC:

      Default glibc - glibc-2.2.4-26
      glibc used for certification - glibc-2.2.4-31.7

- Required Filesytem:

  ext3 (`LARGEFILES` support enabled) filesystem has been used for the certification process.

Installing System Patches

Directory Server has been certified on Red Hat Linux Advanced Server 2.1 with kernel revisions 2.4.9-e.16 (`kernel-2.4.9-e.16.i686.rpm`) / glibc version 2.2.4-31.7 (`glibc-2.2.4-31.7.i686.rpm`). Table 3-3 provides the list of `.rpm` packages that were installed in the test machines during the certification process of this release of Directory Server. (If the machine is a single CPU machine, the corresponding kernel would be of the form `kernel-x.x.x.x`. If the machine is a multi-CPU machine, the corresponding kernel would be of the form `kernel-smp-x.x.x.x`.)

Table 3-3 Red Hat Linux Advanced Server 2.1 Patch List

arts-2.2.2-6.i386.rpm	openssh-askpass-3.1p1-6.i386.rpm
authconfig-4.1.19.2-1.i386.rpm	openssh-askpass-gnome-3.1p1-6.i386.rpm
bind-utils-9.2.1-1.7x.2.i386.rpm	openssh-clients-3.1p1-6.i386.rpm
chkconfig-1.3.5-3.i386.rpm	openssh-server-3.1p1-6.i386.rpm
compat-libstdc++-6.2.rpm	openssl-0.9.6b-30.7.i686.rpm
cpp-2.96-116.7.2.i386.rpm	openssl-0.9.6b-32.7.i386.rpm
cvs-1.11.1p1-8.7.i386.rpm	openssl095a-0.9.5a-18.7.i386.rpm
db3x-3.2.9-3.i386.rpm	openssl095a-0.9.5a-20.7.i386.rpm
file-3.39-8.7x.i386.rpm	openssl096-0.9.6-13.7.i386.rpm
fileutils-4.1-10.1.i386.rpm	openssl096-0.9.6-16.7.i386.rpm
ftp-0.17-12.1.1.i386.rpm	pam-0.75-46.7.3.i386.rpm
gcc-2.96-116.7.2.i386.rpm	passwd-0.68-1.2.1.i386.rpm
gdk-pixbuf-0.14.0-0.2.1.i386.rpm	pax-3.0-4AS.i386.rpm
gdk-pixbuf-gnome-0.14.0-0.2.1.i386.rpm	pwdb-0.62-1.i386.rpm
ghostscript-6.51-16.2.i386.rpm	python-1.5.2-43.72.i386.rpm
glibc-2.2.4-31.7.i686.rpm	redhat-config-network-1.0.4-0.AS21.1.i386.rpm
glibc-common-2.2.4-31.7.i386.rpm	rusers-0.17-20.AS21.2.i386.rpm
glibc-devel-2.2.4-31.7.i386.rpm	rusers-server-0.17-20.AS21.2.i386.rpm
initscripts-6.47.2-1.1.i386.rpm	sendmail-8.11.6-24.72.i386.rpm

Table 3-3 Red Hat Linux Advanced Server 2.1 Patch List *(Continued)*

iputils-20001110-6.AS21.2.i386.rpm	sendmail-8.11.6-26.72.i386.rpm
kde-i18n-Japanese-3.0.3-2.noarch.rpm	sendmail-cf-8.11.6-24.72.i386.rpm
kdebase-2.2.2-6.i386.rpm	sendmail-cf-8.11.6-26.72.i386.rpm
kdelibs-2.2.2-6.i386.rpm	shadow-utils-20000902-9.7.i386.rpm
kdelibs-sound-2.2.2-6.i386.rpm	tar-1.13.25-4.AS21.0.i386.rpm
kdenetwork-2.2.2-3.i386.rpm	tkinter-1.5.2-43.72.i386.rpm
kdepim-2.2.2-4.i386.rpm	unzip-5.50-2.i386.rpm
kdeutils-2.2.2-2.i386.rpm	util-linux-2.11f-20.i386.rpm
kernel-2.4.9-e.16.i686.rpm	vim-common-6.0-7.15.i386.rpm
kernel-headers-2.4.9-e.16.i386.rpm	vim-minimal-6.0-7.15.i386.rpm
kernel-smp-2.4.9-e.16.i686.rpm	vnc-3.3.3r2-18.6.i386.rpm
krb5-libs-1.2.2-24.i386.rpm	vnc-server-3.3.3r2-18.6.i386.rpm
libpcap-0.6.2-12.2.1AS.2.i386.rpm	wget-1.8.2-4.72.i386.rpm
libpng-1.0.14-0.7x.4.i386.rpm	x86-compat-libs-7.2-1.i386.rpm
libstdc++-2.96-116.7.2.i386.rpm	xchat-1.8.9-1.21as.1.i386.rpm
modutils-2.4.13-13.i386.rpm	XFree86-100dpi-fonts-4.1.0-29.i386.rpm
mount-2.11g-6.i386.rpm	XFree86-4.1.0-29.i386.rpm
mozilla-1.0.1-2.2.1.i386.rpm	XFree86-75dpi-fonts-4.1.0-29.i386.rpm
mozilla-nspr-1.0.1-2.2.1.i386.rpm	XFree86-ISO8859-15-100dpi-fonts-4.1.0-29.i386.rpm
netpbm-9.24-9.AS21.2.i386.rpm	XFree86-ISO8859-15-75dpi-fonts-4.1.0-29.i386.rpm
netpbm-progs-9.24-9.AS21.2.i386.rpm	XFree86-libs-4.1.0-29.i386.rpm
nscd-2.2.4-31.7.i386.rpm	XFree86-tools-4.1.0-29.i386.rpm
nss_ldap-189-4.i386.rpm	XFree86-twm-4.1.0-29.i386.rpm
ntp-4.1.0b-2.AS21.4.i386.rpm	XFree86-xdm-4.1.0-29.i386.rpm
ntsysv-1.3.5-3.i386.rpm	XFree86-xfs-4.1.0-29.i386.rpm
openldap-2.0.27-2.7.3.i386.rpm	xpdf-0.92-8.i386.rpm
openldap-clients-2.0.27-2.7.3.i386.rpm	ypserv-1.3.12-2.AS21.i386.rpm
openssh-3.1p1-6.i386.rpm	-

Tuning the System

This section contains some basic system tuning information. Keep in mind that changing any of the following kernel tuning parameters requires a system reboot.

- NFS Tuning—This tuning is recommended if you are using Directory Server to write to NFS mounted drives. On Linux, NFS is typically recommended to be done over TCP and not over UDP. Make the following change to the `/etc/rc.d/init.d/autofs` file:

  ```
  + localoptions='rsize=8192,wsize=8192,vers=3,tcp'
  ```

- TCP Tuning—You can increase number of local system ports available by running this command:

  ```
  echo "1024 65000" > /proc/sys/net/ipv4.ip_local_port_range
  ```

  You can also achive the same by editing this parameter in the `/etc/sysctl.conf` file:

  ```
  [ echo "1024 65000" >> /etc/sysctl.conf ]
  ```

- File Tuning—You can increase the file descriptors by running these commands:

  `echo "64000" > /proc/sys/fs/file-max` or edit this parameter in the `/etc/sysctl.conf` file: `[ echo "fs.file-max = 64000" >> /etc/sysctl.conf ]`

  ```
  echo "* soft nofile 8192" >> /etc/security/limits.conf
  ```

  ```
  echo "* hard nofile 8192" >> /etc/security/limits.conf
  ```

  ```
  echo "ulimit -n 8192" >> /etc/profile
  ```

  ```
  echo "session required /lib/security/pam_limits.so" >>
  /etc/security/limits.conf
  ```

Installing Third-Party Utilities

You will need the `gunzip` utility to unpack the Directory Server software. The GNU `gzip` and `gunzip` programs are described in more detail at `http://www.gnu.org/software/gzip/gzip.html` and can be obtained from many software distribution sites.

You may need Adobe Acrobat Reader to read the documentation. If you do not have it installed, you can download it from: `http://www.adobe.com/products/acrobat/readstep2.html`

Sun Solaris 8 Operating System

If you plan to install Directory Server on a machine running the Solaris 8 operating system (OS), follow the recommendations outlined in these sections:

- Verifying Disk Space Requirements
- Verifying Required System Modules
- Installing Patches
- Tuning the System
- Setting File Descriptors
- Tuning TCP Parameters

In addition to these recommendations, be sure to check the OS vendor's web site for the latest information pertaining to your OS version. For example, you should read the *Solaris Operating Environment Security Sun Blueprint* at `http://www.sun.com/blueprints/0100/security.pdf` for advice on guarding against potential security threats.

Below are two URLs that you may find useful:

`http://docs.sun.com`

`http://sunsolve.sun.com`

Verifying Disk Space Requirements

Ensure that you have sufficient disk space before downloading the software.

Current working directory: 120 MB
Partition containing `/usr/netscape`: 2 GB

Verifying Required System Modules

Directory Server requires the use of a SPARC v8+ or an UltraSPARC (SPARC v9) processor, as these processors include support for high performance and multiprocessor systems. Earlier SPARC processors are not supported.

If you run Directory Server on a 64-bit Sun Solaris 8 UltraSPARC machine, it will run as a 32-bit application.

Installing Patches

You must use Solaris 8 with the Sun recommended patches. The Sun recommended patch clusters can be obtained from your Solaris support representative, or from the `http://sunsolve.sun.com` site.

Solaris patches are generally identified by two numbers, for example 108434-10. The first number (108434) identifies the patch itself. The second number identifies the version of the patch, in the example above the patch is version number 10.

Table 3-4 provides the list of Solaris 8 patches that were used during the testing of this release of Directory Server. You must install these patches on your machine before installing the Directory Server product. (The command "`showrev -p`" will list the patches that have been installed on your machine.)

Also keep in mind that Directory Server provides a utility named `dsktune` that can help you verify whether you have the appropriate patches installed on your system. For details, see "dsktune Utility" on page 37.

In addition to the patches listed in Table 3-4 and the patches identified by the `dsktune` utility, we recommend that you check the operating system vendor's web site for information on installing the latest version of the patch clusters to benefit from the latest fixes.

You will need to reboot your machine after installing the patches.

Table 3-4 Solaris 8 Patch List

108434-10:	32-Bit Shared library patch for C++
108435-10:	64-Bit Shared library patch for C++
108528-19:	SunOS 5.8: kernel update patch
108652-64:	X11 6.4.1: Xsun patch
108725-12:	SunOS 5.8: st driver patch
108727-22:	SunOS 5.8: /kernel/fs/nfs and /kernel/fs/sparcv9/nfs patch
108806-14:	SunOS 5.8: Sun Quad FastEthernet qfe driver
108827-40:	SunOS 5.8: /usr/lib/libthread.so.1 patch
108869-18:	SunOS 5.8: snmpdx/mibiisa/libssasnmp/snmplib patch
108875-13:	SunOS 5.8: c2audit patch
108901-06:	SunOS 5.8: /kernel/sys/rpcmod and /kernel/strmod/rpcmod patch
108919-16:	CDE 1.4: dtlogin patch

Table 3-4 Solaris 8 Patch List *(Continued)*

108949-07:	CDE 1.4: libDtHelp / libDtSvc patch
108968-08:	SunOS 5.8: vol / vold / rmmount / dev_pcmem.so.1 patch
108974-25:	SunOS 5.8: dada, uata, dad, sd and scsi drivers patch
108975-06:	SunOS 5.8: / usr / bin / rmformat and / usr / sbin / format patch
108977-01:	SunOS 5.8: libsmedia patch
108981-10:	SunOS 5.8: / kernel / drv / hme and / kernel / drv / sparcv9 / hme patch
108985-03:	SunOS 5.8: / usr / sbin / in.rshd patch
108987-12:	SunOS 5.8: Patch for patchadd and patchrm
108989-02:	SunOS 5.8: / usr / kernel / sys / acctctl and / usr / kernel / sys / exacctsys patch
108993-13:	SunOS 5.8: nss and ldap patch
108997-03:	SunOS 5.8: libexacct and libproject patch
109007-09:	SunOS 5.8: at / atrm / batch / cron patch
109091-05:	SunOS 5.8: / usr / lib / fs / ufs / ufsrestore patch
109134-27:	SunOS 5.8: WBEM patch
109147-21:	SunOS 5.8: linker patch
109223-02:	SunOS 5.8: kpasswd, libgss.so.1 and libkadm5clnt.so.1 patch
109234-09:	SunOS 5.8: Apache Security and NCA Patch
109238-02:	SunOS 5.8: / usr / bin / sparcv7 / ipcs and / usr / bin / sparcv9 / ipcs patch
109277-03:	SunOS 5.8: / usr / bin / iostat patch
109318-31:	SunOS 5.8: suninstall Patch
109320-06:	SunOS 5.8: LP Patch
109324-05:	SunOS 5.8: sh / jsh / rsh / pfsh patch
109326-10:	SunOS 5.8: libresolv.so.2 and in.named patch
109328-03:	SunOS 5.8: ypserv, ypxfr and ypxfrd patch
109470-02:	CDE 1.4: Actions Patch
109657-09:	SunOS 5.8: isp driver patch
109667-04:	SunOS 5.8: / usr / lib / inet / xntpd and / usr / sbin / ntpdate patch
109783-02:	SunOS 5.8: / usr / lib / nfs / nfsd and / usr / lib / nfs / lockd patch
109793-14:	SunOS 5.8: su driver patch

Table 3-4 Solaris 8 Patch List *(Continued)*

109805-15:	SunOS 5.8: /usr/lib/security/pam_krb5.so.1 patch
109862-03:	X11 6.4.1 Font Server patch
109882-06:	SunOS 5.8: eri header files patch
109885-09:	SunOS 5.8: glm patch
109888-20:	SunOS 5.8: platform drivers patch
109898-05:	SunOS 5.8: /kernel/drv/arp patch
109951-01:	SunOS 5.8: jserver buffer overflow
110075-01:	SunOS 5.8: /kernel/drv/devinfo and /kernel/drv/sparcv9/devinfo patch
110283-06:	SunOS 5.8: mkfs and newfs patch
110286-10:	OpenWindows 3.6.2: Tooltalk patch
110322-02:	SunOS 5.8: /usr/lib/netsvc/yp/ypbind patch
110380-04:	SunOS 5.8: ufssnapshots support, libadm patch
110386-02:	SunOS 5.8: RBAC Feature Patch
110387-03:	SunOS 5.8: ufssnapshots support, ufsdump patch
110453-04:	SunOS 5.8: admintool Patch
110458-02:	SunOS 5.8: libcurses patch
110460-26:	SunOS 5.8: fruid/PICL plug-ins patch
110662-10:	SunOS 5.8: ksh patch
110668-03:	SunOS 5.8: /usr/sbin/in.telnetd patch
110670-01:	SunOS 5.8: usr/sbin/static/rcp patch
110700-01:	SunOS 5.8: automount patch
110723-05:	SunOS 5.8: /kernel/drv/sparcv9/eri patch
110838-06:	SunOS 5.8: /platform/SUNW,Sun-Fire-15000/kernel/drv/sparcv9/axq patch
110842-10:	SunOS 5.8: hpc3130 driver patch for SUNW,Sun-Fire-880
110896-02:	SunOS 5.8: cachefs/mount patch
110898-08:	SunOS 5.8: csh/pfcsh patch
110901-01:	SunOS 5.8: /kernel/drv/sgen and /kernel/drv/sparcv9/sgen patch
110903-05:	SunOS 5.8: edit, ex, vedit, vi and view patch

Table 3-4 Solaris 8 Patch List *(Continued)*

110916-03:	SunOS 5.8: sort patch
110934-11:	SunOS 5.8: pkgtrans, pkgadd, pkgchk and libpkg.a patch
110939-01:	SunOS 5.8: /usr/lib/acct/closewtmp patch
110943-01:	SunOS 5.8: /usr/bin/tcsh patch
110945-07:	SunOS 5.8: /usr/sbin/syslogd patch
110951-03:	SunOS 5.8: /usr/sbin/tar and /usr/sbin/static/tar patch
110957-02:	SunOS 5.8: /usr/bin/mailx patch
111069-01:	SunOS 5.8: bsmunconv overwrites root cron tab if cu created /tmp/root
111071-01:	SunOS 5.8: cu patch
111085-02:	SunOS 5.8: /usr/bin/login patch
111098-01:	SunOS 5.8: ROC timezone should be avoided for political reasons
111111-03:	SunOS 5.8: /usr/bin/nawk patch
111232-01:	SunOS 5.8: patch in.fingerd
111234-01:	SunOS 5.8: patch finger
111293-04:	SunOS 5.8: /usr/lib/libdevinfo.so.1 patch
111299-04:	SunOS 5.8: PPP patch
111310-01:	SunOS 5.8: /usr/lib/libdhcpagent.so.1 patch
111321-03:	SunOS 5.8: klmmod and klmops patch
111325-02:	SunOS 5.8: /usr/lib/saf/ttymon patch
111327-05:	SunOS 5.8: libsocket patch
111504-01:	SunOS 5.8: /usr/bin/tip patch
111548-01:	SunOS 5.8: catman, man, whatis, apropos and makewhatis patch
111570-02:	SunOS 5.8: uucp patch
111596-02:	SunOS 5.8: /usr/lib/netsvc/yp/rpc.yppasswdd patch
111606-02:	SunOS 5.8: /usr/sbin/in.ftpd patch
111626-03:	OpenWindows 3.6.2: Xview Patch
111659-07:	SunOS 5.8: passwd and pam_unix.so.1 patch
111826-01:	SunOS 5.8: /usr/sbin/sparcv7/whodo & /usr/sbin/sparcv9/whodo patch
111874-06:	SunOS 5.8: usr/bin/mail patch

Table 3-4 Solaris 8 Patch List *(Continued)*

111879-01:	SunOS 5.8: Solaris Product Registry patch SUNWwsr
111881-03:	SunOS 5.8: /usr/kernel/strmod/telmod patch
111883-14:	SunOS 5.8: Sun GigaSwift Ethernet 1.0 driver patch
111958-02:	SunOS 5.8: /usr/lib/nfs/statd patch
112138-01:	SunOS 5.8:: usr/bin/domainname patch
112218-01:	SunOS 5.8:: pam_ldap.so.1 patch
112237-07:	SunOS 5.8: mech_krb5.so.1 patch
112254-01:	SunOS 5.8: /kernel/sched/TS patch
112279-02:	SunOS 5.8: pkgrm failed during upgrade from Solaris 8 to Solaris 9 with DSR
112325-01:	SunOS 5.8: /kernel/fs/udfs and /kernel/fs/sparcv9/udfs patch
112396-02:	SunOS 5.8: /usr/bin/fgrep patch
112425-01:	SunOS 5.8: /usr/lib/fs/ufs/mount and /etc/fs/ufs/mount patch
112459-01:	SunOS 5.8: /usr/lib/pt_chmod patch
112611-01:	SunOS 5.8: /usr/lib/libz.so.1 patch
112668-01:	SunOS 5.8: /usr/bin/gzip patch
112796-01:	SunOS 5.8: /usr/sbin/in.talkd patch
112846-01:	SunOS 5.8: /usr/lib/netsvc/rwall/rpc.rwalld patch
113650-01:	SunOS 5.8: /usr/lib/utmp_update patch
113792-01:	OpenWindows 3.6.2: mailtool patch
114152-01:	SunOS 5.8: Japanese SunOS 4.x Binary Compatibility(BCP) patch

Tuning the System

Basic Solaris tuning guidelines are available from several books, including *Sun Performance and Tuning: Java and the Internet (ISBN 0-13-095249-4).* Advanced tuning information is available in the *Solaris Tunable Parameters Reference Manual* (806-4015) which can be obtained from this URL:
`http://docs.sun.com/db/doc/806-4015`

Setting File Descriptors

The system-wide maximum file descriptor table size setting will limit the number of concurrent connections that can be established to Directory Server. The governing parameter, `rlim_fd_max`, is set in the `/etc/system` file. By default, if this parameter is not present, the maximum is 1024. It can be raised to 4096 by adding to `/etc/system` a line

```
set rlim_fd_max=4096
```

and rebooting the system.

CAUTION This parameter should not be raised above 4096 without first consulting your Sun Solaris support representative as it may affect the stability of the system.

You should also set the soft limit for file descriptors:

```
ulimit -n
in csh limit desc 1024
```

Use the `dsktune` utility (see “dsktune Utility” on page 37) to check about the hard and soft limits for file descriptors.

Tuning TCP Parameters

By default, the TCP/IP implementation in a Solaris kernel is not correctly tuned for Internet or Intranet services. The following `/dev/tcp` tuning parameters should be inspected and, if necessary, changed to fit the network topology of the installation environment.

The `tcp_time_wait_interval` in Solaris 8 specifies the number of milliseconds that a TCP connection will be held in the kernel’s table after it has been closed. If its value is above 30000 (30 seconds) and the directory is being used in a LAN, MAN or under a single network administration, it should be reduced by adding a line similar to the following to the `/etc/init.d/inetinit` file:

```
ndd -set /dev/tcp tcp_time_wait_interval 30000
```

The `tcp_conn_req_max_q0` and `tcp_conn_req_max_q` parameters control the maximum backlog of connections that the kernel will accept on behalf of the Directory Server process. If the directory is expected to be used by a large number of client hosts simultaneously, these values should be raised to at least 1024 by adding a line similar to the following to the `/etc/init.d/inetinit` file:

```
ndd -set /dev/tcp tcp_conn_req_max_q0 1024
ndd -set /dev/tcp tcp_conn_req_max_q 1024
```

The `tcp_keepalive_interval` specifies the interval in seconds between keepalive packets sent by Solaris for each open TCP connection. This can be used to remove connections to clients that have become disconnected from the network.

The `tcp_rexmit_interval_initial` value should be inspected when performing server performance testing on a LAN or high speed MAN or WAN. For operations on the wide area Internet, its value need not be changed.

The `tcp_smallest_anon_port` controls the number of simultaneous connections that can be made to the server. When `rlim_fd_max` has been increased to above 4096, this value should be decreased, by adding a line similar to the following to the `/etc/init.d/inetinit` file:

```
ndd -set /dev/tcp tcp_smallest_anon_port 8192
```

The `tcp_slow_start_initial` parameter should be inspected if clients will predominately be using the Windows TCP/IP stack.

Sun Solaris 9 Operating System

If you plan to install Directory Server on a machine running the Solaris 9 operating system (OS), follow the recommendations outlined in these sections:

- Verifying Disk Space Requirements
- Verifying Required System Modules
- Installing Patches
- Tuning the System
- Setting File Descriptors
- Tuning TCP Parameters

In addition to these recommendations, be sure to check the OS vendor's web site for the latest information pertaining to your OS version. For example, you should read the *Solaris Operating Environment Security Sun Blueprint* at `http://www.sun.com/blueprints/0100/security.pdf` for advice on guarding against potential security threats.

Below are two URLs that you may find useful:

`http://docs.sun.com`

http://sunsolve.sun.com

Verifying Disk Space Requirements

Ensure that you have sufficient disk space before downloading the Directory Server software.

Current working directory: 120 MB
Partition containing /usr/netscape: 2 GB

Verifying Required System Modules

Directory Server requires the use of a SPARC v8+ or an UltraSPARC (SPARC v9) processor, as these processors include support for high performance and multiprocessor systems. Earlier SPARC processors are not supported.

If you run Directory Server on a 64-bit Sun Solaris 8 UltraSPARC machine, it will run as a 32-bit application.

Installing Patches

You must use Solaris 9 with the Sun recommended patches. The Sun recommended patch clusters can be obtained from your Solaris support representative, or from the http://sunsolve.sun.com site.

Solaris patches are identified by two numbers, for example 112233-04. The first number (112233) identifies the patch itself. The second number identifies the version of the patch, in the example above the patch is version number 04.

Table 3-5 provides the list of Solaris 9 patches that were used during the testing of this release of Directory Server. You must install these patches on your machine before installing the Directory Server product. (The command "showrev -p" will list the patches that have been installed on your machine.)

Also keep in mind that Directory Server provides a utility named dsktune that can help you verify whether you have the appropriate patches installed on your system. For details, see "dsktune Utility" on page 37.

In addition to the patches listed in Table 3-5 and the patches identified by the dsktune utility, we recommend that you check the operating system vendor's web site for information on installing the latest version of the patch clusters to benefit from the latest fixes.

You will need to reboot your machine after installing the patches.

Table 3-5 Solaris 9 Patch List

112233-04:	SunOS 5.9: Kernel Patch
112601-04:	SunOS 5.9: PGX32 Graphics
112764-04:	SunOS 5.9: Sun Quad FastEthernet qfe driver
112785-12:	X11 6.6.1: Xsun patch
112808-03:	OpenWindows 3.6.3: Tooltalk patch
112817-06:	SunOS 5.9: Sun GigaSwift Ethernet 1.0 driver patch
112834-02:	SunOS 5.9: patch scsi
112875-01:	SunOS 5.9: patch /usr/lib/netsvc/rwall/rpc.rwalld
112902-08:	SunOS 5.9: kernel/drv/ip Patch
112907-01:	SunOS 5.9: libgss Patch
112908-07:	SunOS 5.9: gl_kmech_krb5 Patch
112951-04:	SunOS 5.9: patchadd and patchrm Patch
112963-05:	SunOS 5.9: linker patch
112964-02:	SunOS 5.9: ksh using control Z under ksh does not work well with vi
112970-02;	SunOS 5.9: patch libresolv.so.2
112998-02:	SunOS 5.9: patch /usr/sbin/syslogd
113023-01:	SunOS 5.9: Broken preremove scripts in S9 ALC packages
113033-03:	SunOS 5.9: patch /kernel/drv/isp and /kernel/drv/sparcv9/isp
113068-01:	SunOS 5.9: hpc3130 patch
113146-01:	SunOS 5.9: Apache Security Patch
113273-01:	SunOS 5.9: /usr/lib/ssh/sshd Patch
113277-04:	SunOS 5.9: sd and ssd Patch
113278-01:	SunOS 5.9: NFS Daemon Patch
113279-01:	SunOS 5.9: klmmod Patch
113319-05:	SunOS 5.9: patch /usr/lib/libnsl.so.1
113333-02:	SunOS 5.9: libmeta Patch
113492-01:	SunOS 5.9: fsck Patch
113579-01:	SunOS 5.9: ypserv/ypxfrd Patch
113718-01:	SunOS 5.9: usr/lib/utmp_update Patch

Table 3-5 Solaris 9 Patch List *(Continued)*

113923-02:	X11 6.6.1: security font server patch
113993-01:	SunOS 5.9: mkfs Patch
114135-01:	SunOS 5.9: at utility Patch

Tuning the System

Basic Solaris tuning guidelines are available from several books, including *Sun Performance and Tuning: Java and the Internet (ISBN 0-13-095249-4)*. Advanced tuning information is available in the *Solaris Tunable Parameters Reference Manual* (816-7137), which can be obtained from this URL:
`http://docs.sun.com/db/doc/816-7137`

Setting File Descriptors

The system-wide maximum file descriptor table size setting will limit the number of concurrent connections that can be established to Directory Server. The governing parameter, `rlim_fd_max`, is set in the `/etc/system` file. By default, if this parameter is not present, the maximum is 1024. It can be raised to 4096 by adding to `/etc/system` a line

```
set rlim_fd_max=4096
```

and rebooting the system.

CAUTION This parameter should not be raised above 4096 without first consulting your Sun Solaris support representative as it may affect the stability of the system.

You should also set the soft limit for file descriptors:

```
ulimit -n
in csh limit desc 1024
```

Use the `dsktune` utility (see “dsktune Utility” on page 37) to check about the hard and soft limits for file descriptors.

Tuning TCP Parameters

By default, the TCP/IP implementation in a Solaris kernel is not correctly tuned for Internet or Intranet services. The following `/dev/tcp` tuning parameters should be inspected and, if necessary, changed to fit the network topology of the installation environment.

The `tcp_time_wait_interval` in Solaris 9 specifies the number of milliseconds that a TCP connection will be held in the kernel's table after it has been closed. If its value is above 30000 (30 seconds) and the directory is being used in a LAN, MAN or under a single network administration, it should be reduced by adding a line similar to the following to the `/etc/init.d/inetinit` file:

```
ndd -set /dev/tcp tcp_time_wait_interval 30000
```

The `tcp_conn_req_max_q0` and `tcp_conn_req_max_q` parameters control the maximum backlog of connections that the kernel will accept on behalf of the Directory Server process. If the directory is expected to be used by a large number of client hosts simultaneously, these values should be raised to at least 1024 by adding a line similar to the following to the `/etc/init.d/inetinit` file:

```
ndd -set /dev/tcp tcp_conn_req_max_q0 1024
ndd -set /dev/tcp tcp_conn_req_max_q 1024
```

The `tcp_keepalive_interval` specifies the interval in seconds between keepalive packets sent by Solaris for each open TCP connection. This can be used to remove connections to clients that have become disconnected from the network.

The `tcp_rexmit_interval_initial` value should be inspected when performing server performance testing on a LAN or high speed MAN or WAN. For operations on the wide area Internet, its value need not be changed.

The `tcp_smallest_anon_port` controls the number of simultaneous connections that can be made to the server. When `rlim_fd_max` has been increased to above 4096, this value should be decreased, by adding a line similar to the following to the `/etc/init.d/inetinit` file:

```
ndd -set /dev/tcp tcp_smallest_anon_port 8192
```

The `tcp_slow_start_initial` parameter should be inspected if clients will predominately be using the Windows TCP/IP stack.

DNS and NIS Requirements (UNIX Only)

Prior to installation, it is necessary to have configured the DNS resolver and NIS domain name.

The DNS resolver is typically set by the file `/etc/resolv.conf`. However, also check the file `/etc/nsswitch.conf`, and on Solaris `/etc/netconfig`, to ensure that the DNS resolver will be used for name resolution.

If you are not already using NIS, you will also need to set the default NIS domain name. Typically this is done by placing the NIS domain name in the file `/etc/defaultdomain` and rebooting or by using the `domainname` command.

Chapter 4

Silent Installation and Instance Creation

Silent installation allows you to use a file to predefine all the answers that you would normally supply to the `setup` program interactively; this provides you with the ability to script the installation of multiple instances of Netscape Directory Server (Directory Server). Instance creation enables you to use an existing Directory Server instance to create additional instances of the server under the same server root.

This chapter explains the following:

- Using Silent Installation (page 67)
- Using Silent Instance Creation (page 79)

Using Silent Installation

Silent installation is intended for use at sites where many server instances must be created. For Directory Server, it is especially useful for heavily replicated sites that will create a large number of consumer servers.

To use silent installation, you create a silent installation file, supply values for the appropriate installation directives, and run the `setup` program with the `-s` and `-f` command-line options.

The procedure below explains how to use silent installation:

1. On Windows machines, log in with `Administrator` privileges. On UNIX machines, log in as `root`.

2. Create a new directory:

   ```
   # mkdir ds
   # cd ds
   ```

3. If you have not already done so, download the product binaries file to the installation directory.

4. On Windows machines, unzip the product binaries. On UNIX, unpack the product binaries file using the following command:

   `# gunzip -dc` *filename*`.tar.gz | tar -xvof-`

   where *filename* corresponds to the product binaries file that you want to unpack.

5. Prepare the file that will contain your installation directives.

   See “Preparing Silent Installation Files” on page 68 for instructions and for some examples of the silent-install files.

6. Fill in appropriate values for the installation directives.

   See “Specifying Silent Installation Directives” on page 73 for the complete list of silent installation directives that you can use when installing Directory Server.

7. Run the `setup` program with the `-s` and `-f` command line options:

   `setup -s -f` *filename*

   where *filename* is the name of the file that contains your installation directives.

Preparing Silent Installation Files

The best way to create a file for use with silent installation is to use the `setup` program to interactively create a server instance of the type that you want to duplicate. To do this, run `setup` with the `-k` flag. The `setup` program will create the following file:

serverRoot`/setup/install.inf`

This file contains all the directives that you would use with silent installation to create the server instance. You can then use this file to create other server instances of that type.

You will have to make some modifications to this file before you use it. Specifically, ensure that you have done the following:

- `FullMachineName`—Set this directive to a value that is appropriate for the machine on which Directory Server will be installed, if it's not to be the local machine. In most circumstances, it is best not to use this directive because `FullMachineName` will then default to the local host name. However, if you use custom installation to generate your initial server instance, then this directive will appear in the `install.inf` file.
- `ServerIpAddress`—Set this directive appropriate for the local machine. The same usage rules apply for `ServerIpAddress` as for `FullMachineName`. Specifically, try to not include `ServerIpAddress` in your `install.inf` file unless you absolutely have to (as may be necessary for multi-homed systems).
- `ServerRoot`—Verify the installation path on this directive. If you are installing on both Windows and UNIX machines, make sure the appropriate path delimiter is used. Add or remove the Windows drive letter designation as is appropriate for the host you are installing on. Also, the name of the file-system directory where you install files must not contain any space characters.
- `ServerIdentifier`—If you are installing more than one Directory Server on the same host, make sure that this directive contains a unique value for each server instance.
- `SuiteSpotUserID` and `SuiteSpotGroup`—If you create your `install.inf` file on a Windows machine, then the `SuiteSpotUserID` and `SuiteSpotGroup` directives are both set to `nobody`. If you subsequently use this file on a UNIX machine, ensure the user and group specified by these directives are appropriate for the machine. The `SuiteSpotUserID` and `SuiteSpotGroup` directives determine what user and group a server will run under when installed on a UNIX system.

NOTE Be sure to protect your `install.inf` files because they contain passwords in clear. Also ensure that any DNs in these files are in the UTF-8 character set encoding.

The sections that follow provide examples of using silent installation to support the following installation scenarios:

- Sample File for Typical Installation
- Sample File for Using an Existing Configuration Directory
- Sample File for Installing the Standalone Netscape Console

You can find a definition of the individual installation directives in “Specifying Silent Installation Directives” on page 73.

NOTE The `silent.inf` file provided with the Directory Server is merely a template, an example of how to write your own. For the file to work, many of the parameters (host name, ports, paths, and so on) in the file must be replaced with appropriate values.

It is also easy to generate your own silent installation file using the `setup -k` option, and modify the resulting `install.inf` file as needed.

Sample File for Typical Installation

The following is an example of the `install.inf` file that is generated for a typical installation:

```
[General]
FullMachineName= dir.example.com
SuiteSpotUserID= nobody
SuiteSpotGroup= nobody
ServerRoot= /usr/netscape/servers
AdminDomain= example.com
ConfigDirectoryAdminID= admin
ConfigDirectoryAdminPwd= admin
ConfigDirectoryLdapURL= ldap://dir.example.com:389/o=NetscapeRoot
UserDirectoryAdminID= admin
UserDirectoryAdminPwd= admin
UserDirectoryLdapURL=
ldap://dir.example.com:389/dc=example,dc=com
Components= svrcore,base,slapd,admin,nsperl,perldap

[slapd]
SlapdConfigForMC= Yes
SecurityOn= No
UseExistingMC= No
UseExistingUG= No
ServerPort= 389
ServerIdentifier= dir
Suffix= dc=example,dc=com
RootDN= cn=Directory Manager
UseReplication= No
AddSampleEntries= No
InstallLdifFile= suggest
AddOrgEntries= Yes
DisableSchemaChecking= No
RootDNPwd= admin123
Components= slapd,slapd-client
```

```
[admin]
SysUser= root
Port= 23611
ServerIpAddress= 111.11.11.11
ServerAdminID= admin
ServerAdminPwd= admin
Components= admin,admin-client

[base]
Components= base,base-client,base-jre

[nsperl]
Components= nsperl561

[perldap]
Components= perldap14
```

Sample File for Using an Existing Configuration Directory

The following is an example of the `install.inf` file that is generated when you perform a typical installation and you choose to use an existing Directory Server as the configuration directory:

```
[General]
FullMachineName= dir.example.com
SuiteSpotUserID= nobody
SuiteSpotGroup= nobody
ServerRoot= /usr/netscape/servers
AdminDomain= example.com
ConfigDirectoryAdminID= admin
ConfigDirectoryAdminPwd= admin
ConfigDirectoryLdapURL=
ldap://dir.example.com:25389/o=NetscapeRoot
UserDirectoryLdapURL=
ldap://dir.example.com:18257/dc=example,dc=com
UserDirectoryAdminID= cn=Directory Manager
UserDirectoryAdminPwd= admin123
Components= svrcore,base,slapd,admin,nsperl,perldap

[slapd]
SlapdConfigForMC= No
SecurityOn= No
UseExistingMC= Yes
UseExistingUG= No
ServerPort= 18257
ServerIdentifier= directory
Suffix= dc=example,dc=com
RootDN= cn=Directory Manager
UseReplication= No
```

```
AddSampleEntries= No
InstallLdifFile= suggest
AddOrgEntries= Yes
DisableSchemaChecking= No
RootDNPwd= admin123
Components= slapd,slapd-client

[admin]
SysUser= root
Port= 33646
ServerIpAddress= 111.11.11.11
ServerAdminID= admin
ServerAdminPwd= admin
Components= admin,admin-client

[base]
Components= base,base-client,base-jre

[nsperl]
Components= nsperl561

[perldap]
Components= perldap14
```

Sample File for Installing the Standalone Netscape Console

The following is an example of the `install.inf` file that is generated when you install just Netscape Console:

```
[General]
FullMachineName= dir.example.com
ConfigDirectoryLdapURL= ldap://dir.example.com:389/o=NetscapeRoot
SuiteSpotUserID= nobody
SuiteSpotGroup= nobody
ConfigDirectoryAdminID= admin
ConfigDirectoryAdminPwd= admin
ServerRoot= /usr/netscape/servers
Components= svrcore,base,slapd,admin

[base]
Components= base-client

[slapd]
Components= slapd-client

[admin]
Components= admin-client,base-jre
```

Specifying Silent Installation Directives

This section describes the basic format of the file used for silent installation. It then describes the directives that are available for each area of the silent installation file.

- Silent Installation File Format
- [General] Installation Directives
- [slapd] Installation Directives
- [admin] Installation Directives
- [Base] Installation Directives
- [nsperl] Installation Directives
- [perldap] Installation Directives

Silent Installation File Format

When you use silent installation, you provide all the installation information in a file. This file is formatted as follows:

```
[General]
directive=value
directive=value
directive=value
...
[slapd]
directive=value
directive=value
directive=value
...
[admin]
directive=value
directive=value
directive=value
...
[Base]
directive=value
directive=value
directive=value
...
```

The keywords `[General]`, `[slapd]`, and `[admin]` are required. They indicate that the directives that follow are meant for a specific aspect of the installation. They must be provided in the file in the order indicated above.

[General] Installation Directives

[General] installation directives specify information of global interest to the Netscape servers installed at your site. That is, the information you provide here will be common to all your Netscape servers.

The [General] installation directives are listed in Table 4-1.

Table 4-1 [General] Installation Directives

Directive	Description
`Components`	Specifies components to be installed. The list of available components will differ depending on the Netscape servers available on your installation media. For standalone directory installation, the list of components is: • `svrcore`—Uninstallation binaries • `base`—The base installation package • `admin`—The Administration Server binaries • `slapd`—The Directory Server binaries This directive is required. At a minimum, you should always provide: `components= svrcore,base,admin`
`ServerRoot`	Specifies the full path to the directory where the Netscape server binaries are installed. This directive is required.
`FullMachineName`	Specifies the fully qualified domain name of the machine on which you are installing the server. The default is the local host name.
`SuiteSpotUserID`	UNIX only. Specifies the user name that Netscape servers will run as. This parameter does not apply to the user that the Administration Server runs as. See the `SysUser` directive in Table 4-3 for more information. The default is user `nobody` but this should be changed for most deployments.
`SuiteSpotGroup`	UNIX only. Specifies the group that Netscape servers will run as. The default is group `nobody` but this should be changed for most deployments.

Table 4-1 [General] Installation Directives *(Continued)*

Directive	Description
`ConfigDirectoryLdapURL`	Specifies the LDAP URL that is used to connect to your configuration directory. LDAP URLs are described in the *Netscape Directory Server Administrator's Guide.* This directive is required.
`AdminDomain`	Specifies the administration domain under which this server will be registered. See "Determining the Administration Domain" on page 18 for more information about administration domains.
`ConfigDirectoryAdminID`	Specifies the user ID of the entry that has administration privileges to the configuration directory. This directive is required.
`ConfigDirectoryAdminPwd`	Specifies the password for the `ConfigDirectoryAdminID`. This directive is required.
`UserDirectoryLdapURL`	Specifies the LDAP URL that is used to connect to the directory where your user and group data is stored. If this directive is not supplied, the configuration directory is used for this purpose. LDAP URLs are described in the *Netscape Directory Server Administrator's Guide.*
`UserDirectoryAdminID`	Specifies the user ID of the entry that has administration privileges to the user directory.
`UserDirectoryAdminPwd`	Specifies the password for the `UserDirectoryAdminID`.

[slapd] Installation Directives

[slapd] installation directives specify information of interest only to the Directory Server instance that you are currently installing. These directives are classified as follows:

- Required [slapd] Installation Directives—You must provide these directives when you use silent installation with Directory Server.
- Optional [slapd] Installation Directives—You may provide these directives when you use silent installation with Directory Server.

Table 4-2 lists the directives.

Table 4-2 Required and Optional [slapd] Installation Directives

Required Directive	Description
`Components`	Specifies the `slapd` components to be installed. The components are: • `slapd`—Install Directory Server. • `slapd-client`—Install Directory Server Console. This directive is required. It is recommended that you always install both components any time you install the Directory Server.
`ServerPort`	Specifies the port the server will use for LDAP connections. For information on selecting server port numbers, see "Choosing Unique Port Numbers" on page 13. This directive is required.
`ServerIdentifier`	Specifies the server identifier. This directive is required. This value is used as part of the name of the directory in which the Directory Server instance is installed. For example, if your machine's host name is `phonebook`, then this name is the default and selecting it will cause the Directory Server instance to be installed into a directory labeled `slapd-phonebook`.
`Suffix`	Specifies the suffix under which you will store your directory data. For information on suffixes, see "Determining Your Directory Suffix" on page 16. This directive is required.
`RootDN`	Specifies the distinguished name used by the directory manager. For information on the directory manager, see "Defining Authentication Entities" on page 15. This directive is required.
`RootDNPwd`	Specifies the directory manager's password. This directive is required.
Optional Directive	**Description**
`AddSampleEntries`	If set to `Yes`, this directive causes the `example.ldif` sample directory to be loaded. Use this directive if you are installing the Directory Server for evaluation purposes and you do not already have an LDIF file to populate your directory with. Default is `no`.

Table 4-2 Required and Optional [slapd] Installation Directives *(Continued)*

Required Directive	Description
`AddOrgEntries`	If set to `Yes`, this directive causes the new Directory Server instance to be created with a suggested directory structure and access control. If this directive is used and `InstallLdifFile` is also used, then this directive has no effect. Default is `no`.
`InstallLdifFile`	Causes the contents of the LDIF file to be used to populate your directory.

[admin] Installation Directives

[admin] installation directives specify information of interest only to your Directory Server's Administration Server. That is, this is the installation information required for the Administration Server that is used to manage the Directory Server instance that you are currently installing.

The [admin] installation directives are listed in Table 4-3.

Table 4-3 [admin] Installation Directives

Directive	Description
`Components`	Specifies the admin components to be installed. The base components are: • `admin`—Install Administration Server. You must install the Administration Server if you are also installing some other Netscape server. • `admin-client`—Install Netscape Console. Specify just this component if you are installing Netscape Console as stand-alone. Do not install this component if you will remotely manage your servers and Netscape Console will be installed somewhere else on your network.
`SysUser`	UNIX only. Specifies the user that the Administration Server will run as. For default installations that use the default Netscape port numbers, this user must be root. Root is the default. For information on what users your servers should run as, see "Deciding the User and Group for Your Netscape Servers (UNIX only)" on page 14

Table 4-3 [admin] Installation Directives *(Continued)*

Directive	Description
`Port`	Specifies the port that the Administration Server will use. Note that the Administration Server's host name is given by the `FullMachineName` directive. For more information on `FullMachineName`, see Table 4-1.
`ServerAdminID`	Specifies the administration ID that can be used to access this Administration Server if the configuration directory is not responding. The default is to use the value specified by the `ConfigDirectoryAdminID` directive. See "Defining Authentication Entities" on page 15 for information on this directive.
`ServerAdminPwd`	Specifies the password for `ServerAdminID`.
`ServerIpAddress`	Specifies the IP address that the Administration Server will listen to. Use this directive if you are installing on a multi-homed system and you do not want to use the first IP address for your Administration Server.

[Base] Installation Directives

There is only one [Base] installation directive and it allows you to determine whether Netscape Console is installed. Table 4-4 lists the directive.

Table 4-4 [Base] Installation Directive

Directive	Description
`Components`	Specifies the base components to be installed. The base components are: • `base`—Install the shared libraries used by all Server Consoles. You must install this package if you are also installing some other Netscape server. • `base-client`—Install the Java run time environment used by the Server Consoles. • `base-jre`—Causes the Java run time environment to be installed. This directive is required if you are installing an Netscape server (versus, for example, just Netscape Console). You must install both packages when you are installing an Netscape server.

[nsperl] Installation Directives

There is only one [nsperl] installation directive and it allows you to determine whether nsPerl is to be installed. Table 4-5 lists the directive.

Table 4-5 [nsperl] Installation Directive

Directive	Description
`Components`	Specifies whether nsPerl that is bundled with Directory Server is to be installed. This nsPerl is CPAN perl, built and maintained for use by Netscape server products. • `nsperl561`—Install nsPerl version 5.6.1. This directive is required if you are installing a Netscape server (versus, for example, just Netscape Console).

[perldap] Installation Directives

There is only one [perldap] installation directive and it allows you to determine whether PerLDAP is to be installed. Table 4-6 lists the directive.

Table 4-6 [perldap] Installation Directive

Directive	Description
`Components`	Specifies whether PerLDAP that is bundled with Directory Server is to be installed. This is `mozilla.org` PerLDAP, built and maintained at Netscape and used by Netscape server products. • `perldap14`—Install perLDAP version 1.4.1. This directive is required if you are installing a Netscape server (versus, for example, just Netscape Console).

Using Silent Instance Creation

If you have Directory Server installed in a server root, you can create additional instances of Directory Server under the same server root without having to run the `setup` program. You can create additional instances of the server either by using Netscape Console or from the command line.

Because all instances of Directory Server under a server root use the same Administration Server, the instance creation process does not install Administration Server binaries; you cannot create two instances of Administration Server in one server root.

Having multiple instances in a single server root is useful for testing and for when one host is used for multiple purposes. Keep in mind that each Directory Server instance must be assigned a different port number and server identifier.

The `ds_create` program, which is located in the *serverRoot*`/bin/slapd/admin/bin` directory, enables you to create additional instances of Directory Server under a server root. You may want to use this program when you already have Directory Server installed and just want to create additional instances of the server from the command line.

To create a new instance of Directory Server, run this command from the *serverRoot*`/bin/slapd/admin/bin` directory:

`ds_create -f` *filename*

where *filename* is the silent instance creation file, which must be similar to the file used with the `setup` program (see “Preparing Silent Installation Files” on page 68) except that the file must only contain the following two sections, and these sections do not take Components directive.

- `[Genaral]`
- `[slapd]`

Here’s a sample file for instance creation:

```
[General]
FullMachineName= testDir.example.com
ServerRoot= /usr/netscape/servers
AdminDomain= example.com
ConfigDirectoryAdminID= admin
ConfigDirectoryAdminPwd= secretPwd01
ConfigDirectoryLdapURL=
ldap://testDir.example.com:389/o=NetscapeRoot
UserDirectoryAdminID= admin
UserDirectoryAdminPwd= secretPwd02
UserDirectoryLdapURL=
ldap://testDir.example.com:389/dc=europe,dc=example,dc=com

[slapd]
ServerPort= 389
ServerIdentifier= instance02
RootDN= cn=Directory Manager
RootDNPwd= DirMgrPwd
Suffix= dc=europe,dc=example,dc=com
```

```
SlapdConfigForMC= No
UseExistingMC= Yes
UseExistingUG= No
SecurityOn= No
UseReplication= No
SetupSupplier= No
SetupConsumer= No
AddSampleEntries= No
InstallLdifFile= suggest
AddOrgEntries= Yes
DisableSchemaChecking= No
```

Chapter 5

Post Installation

This chapter describes the post-installation procedures for launching the online help and populating the directory tree.

This chapter has the following sections:

- Launching the Help System (page 83)
- Populating the Directory Tree (page 84)

Launching the Help System

The help system for Directory Server is dependent upon Netscape Administration Server. If you are running Directory Server Console on a machine remote to Administration Server, you will need to confirm the following:

Client IP address authorized on Administration Server. The machine running Directory Server Console needs access to Administration Server. To configure Administration Server to accept the client machine's IP address, do the following in Administration Server:

1. Launch Administration Server Console. The console should be running on the same machine as Administration Server.
2. Click the Configuration tab, then click the Network tab.
3. In the Connection Restrictions Settings, select "IP Addresses to Allow" from the pull down menu. Click Edit.
4. Edit the IP Addresses field to the following: *.*.*.*

   This allows all clients access to Administration Server.

5. Restart Administration Server. You can now launch the online help by clicking any of the Help buttons in the Directory Server Console.

Proxy authorized on Administration Server. If you use proxies for your HTTP connections on the client machine running Directory Server Console, you need to do one of the following:

- Remove proxies on the machine running Directory Server Console. This allows the client machine to access Administration Server directly.

  To remove the proxies on the machine running Directory Server Console, you need to alter the proxy configuration of the browser you will use to run the help. In Netscape Communicator, select Preferences from the Edit menu. Select Advanced then Proxies to access the proxy configuration. In Internet Explorer, select Internet Options from the Tools menu.

- Add the client machine proxy IP address to Administration Server list of acceptable IP addresses.

CAUTION Adding the client machine proxy IP address to Administration Server creates a potential security hole in your system.

Populating the Directory Tree

During installation, a simple directory database was created for you. In addition, a simple directory structure was placed in the database for you to use. This directory structure contained basic access control and the major branch points for the recommended directory structure.

Now you need to populate your database with user entries. There are several ways you can create and populate your directory suffixes. These are explained in detail in the *Netscape Directory Server Administrator's Guide.*

The main methods are:

- Create a database from LDIF—Use this method if you want to use the sample directory data shipped with Directory Server, if you are importing entries from another directory via LDIF, or if you have more than a few entries to add at once. For more information about LDIF, refer to the *Netscape Directory Server Administrator's Guide.*

- Start your Directory Server with an empty database and import data over LDAP—This method requires you to populate your directory using an LDAP client such as Directory Server Gateway or the `ldapmodify` command-line utility. Use this method if you have just a few entries to add at a time. For information on setting up the Directory Server Gateway, check the *Netscape Directory Server Gateway Customization Guide*. This document is provided with *Netscape Directory Server Resource Kit*.

As you are populating your directory, consider your access control needs and set access control accordingly. For more information on access control, see the *Netscape Directory Server Deployment Guide* and the *Netscape Directory Server Administrator's Guide.*

Chapter 6

Migrating and Upgrading From Previous Versions

If you have a previous installation of Directory Server, depending on it's version, you can migrate or upgrade to Netscape Directory Server 6.x. *Migration* refers to the process of migrating Directory Server 4.x or 5.x files to Directory Server 6.x. *Upgrade* refers to the process of updating Directory Server 6.0x files to Directory Server 6.x.

This chapter covers the migration and upgrade processes in these sections:

- Migration Overview (page 87)
- Migration Prerequisites (page 88)
- Migration Procedure (page 91)
- Upgrading From Directory Server 6.x Versions (page 106)

This chapter does not explain how to upgrade from Innosoft Distributed Directory Server 4.5.1. That process is described in the *Innosoft Distributed Directory Server Transition Guide*.

Migration Overview

Before you migrate your directory service, you should become familiar with the new features offered in this release of the Directory Server.

The migration process is performed by running the `migrateInstance6` script on the system where your legacy Directory Server is installed. You must shut down your directory service before running the migration script.

The migration script performs the following tasks in sequence:

- Checks the schema configuration files and notifies you of any changes between the standard configuration files and the ones present on your system; see
- Creates a database for each suffix stored in the legacy Directory Server. (In Directory Server 5.x and 6.x you can have multiple databases, but just one suffix per database).
- Checks if any database exists and if it does, gives you the option to save the database (by exporting it to a file), skip the database, or overwrite the database.
- Migrates the server parameters and database parameters. (In Directory Server 5.x and 6.x, these are stored as LDAP entries in the `dse.ldif` file.)
- Migrates user-defined schema objects.
- Migrates indexes.
- Migrates standard server plug-ins.
- Migrates the certificate database and SSL parameters.
- Migrates database links.
- Migrates replication entries (change log).
- Migrates the SNMP configuration.

The migration script shuts down your legacy Directory Server before performing the migration process. The migration script also backs up your current configuration.

Migration Prerequisites

This section lists the prerequisites that your system must meet before you can consider beginning the migration process.

- You must be using Directory Server 4.x or 5.x. When you run the migration script, the legacy server process `ns-slapd` should be stopped. (If you don't stop the server, the migration script stops it.)
- Your legacy Directory Server and your new Directory Server must be installed on the same host; migration cannot occur over networked drives.

- Do not install the new Directory Server on top of an existing Directory Server installation. Install your new Directory Server in a separate directory. Migrate your legacy directory data into your new directory and when you are satisfied with the result of the migration, remove your legacy Directory Server.
- If you want to continue to run your legacy Directory Server, when you install the new Directory Server choose different ports for LDAP traffic and for secured connections from the ones used by your legacy Directory Server.

  If you will not be running your legacy Directory Server, use the same port numbers to ensure that any directory clients that have static configuration information (including Directory Server port numbers) will continue to work.
- Your new Directory Server must be running when you execute the migration script.
- Any custom schema that you created in a legacy 4.x Directory Server must be stored in the default files or included using an include statement in the `slapd.conf` file. The default files for custom schema are `slapd.user_oc.conf` and `slapd.user_at.conf files` in Directory Server 4.x. If you have custom schema that is not stored in those files, refer to the procedure described in “Identifying Custom Schema” on page 90” to move it to those files.
- Any custom schema that you created in a 5.x Directory Server must be stored in an LDIF file in the *serverRoot*`/slapd-`*serverID*`/config/schema` directory.
- Before performing the migration, check that the user-defined variables contain the following associated values, where *server6Root* is the path to where your new, Directory Server 6.x is installed:

  On UNIX, set the following environment variables:

  ```
  PERL5LIB=server6Root/bin/slapd/admin/bin
  PATH=server6Root/bin/slapd/admin/bin:$PATH
  ```

  On Windows, set the following environment variables:

  ```
  PERL5LIB=server6Root\bin\slapd\admin\bin
  PATH=server6Root\bin\slapd\admin\bin
  ```

- Windows only. If you are migrating a Directory Server 5.x multi master replicated (MMR) environment to Directory Server 6.2, before you run the migration script, export all exports from the old server's backend databases using the `db2ldif -r` option.
- When you run the migration script, it migrates the configuration files or configuration entries, database instances, and schema with minimum manual intervention. For complete information on the configuration parameters and attributes that are migrated, check chapter "Migration from Earlier Versions" of the *Netscape Directory Server Configuration, Command, and File Reference*.
- Check the command syntax for the migration script in chapter "Command-Line Scripts" of the *Netscape Directory Server Configuration, Command, and File Reference.*

Identifying Custom Schema

If you customized the schema in your legacy Directory Server by modifying `slapd.at.conf` or `slapd.oc.conf` directly, then the server migration process cannot migrate your custom schema for you. Instead, you are notified during migration that you have modified the standard schema and that you need to manually fix the problem. The migration process then saves a copy of your schema files and uses standard legacy schema files in their place.

While the migration will complete in this situation, you will probably find that you cannot modify your data in Directory Server 6.x. Therefore, you are strongly recommended to copy your custom schema into separate files before you perform the migration. You can use the standard `slapd.user_oc.conf` and `slapd.user_at.conf` files or any files declared in `slapd.conf` with the `useroc` and `userat` keywords respectively. Make these changes with the server shut down.

To separate your custom schema from your standard schema:

1. Examine your old `slapd.at.conf` and `slapd.oc.conf` files to discover all the schema additions that you made there.

   To ensure that you have properly identified all your changes to standard files, you can compare them with the standard files provided in the `/bin/slapd/install/version4` directory. Alternatively, if you have already tried to run the `migrateInstance6` script, use the notifications that it issues.

2. Move your custom schema elements to the following files:

   serverRoot/slapd-*serverID*/config/slapd.user_at.conf and *serverRoot*/slapd-*serverID*/config/slapd.user_oc.conf

   These file names are recommended because the 4.x schema configuration editor writes to them. However, you can use any file name you like.

   Note that if there are inheritance relationships between custom defined object classes, you must ensure that in the order in which they appear in the schema configuration file, the superior object class is defined before the others.

3. Include these files into your slapd.conf file using the userat and useroc directives. Place your new directives at the same place in the file as the include statements for other configuration files.

   The order in which the various configuration files are included is not important. Then, if you added custom attributes to standard object classes in slapd.oc.conf, you must do the following:

   a. In the slapd.user_oc.conf file (or your equivalent), create a new object class that includes your custom attributes.

   b. Add this new object class to every entry in your directory that uses the custom attributes.

Migration Procedure

Before you start with migration process, ensure the following:

- Read sections “Migration Overview” on page 87 and “Migration Prerequisites” on page 88.
- The migration script will automatically back up your Directory Server configuration, if it’s in the default location.
  - If you are migrating from Directory Server 4.x, all of the files with a .conf extension in the /usr/netscape/server4/slapd-*serverID* directory are backed up.
  - If you are migrating from Directory Server 5.x, all of the configuration files in the /usr/netscape/servers/slapd-*serverID*/config directory will be backed up to a directory named *serverRoot*/slapd-*serverID*/config_backup.

  If your configuration files are stored in non-default locations, before you migrate your server, copy them to a secure place.

This section contains the following information:

- Migrating a Standalone Server
- Migrating a 4.x Replicated Site
- Migrating a 5.x Replicated Site
- Migrating a 5.x Multi-Master Deployment
- Managing Console Fail Over

Migrating a Standalone Server

Once you have backed up your critical configuration information, do the following to migrate a server:

1. Stop your legacy Directory Server.

   If you do not stop the legacy Directory Server, the migration script does it for you.

2. On the machine where your legacy Directory Server is installed, install a new, 6.x Directory Server.

   The installation process is described in Chapter 2, “Using Express and Typical Installation” or Chapter 4, “Silent Installation and Instance Creation.”

   Use the same port numbers as your legacy production server if you want to ensure that any directory clients that have static configuration information (including Directory Server port numbers) will continue to work.

3. Run the migration script.

   As *root* user (on UNIX) or *administrator* (on Windows), change directory to *serverRoot*`/bin/slapd/admin/bin`. Then enter the following command:

   On UNIX:

   `migrateInstance6 -D` *rootDN* `-w` *password* `-p` *port* `-o` *oldInstancePath* `-n` *newInstancePath*

   On Windows:

   `perl migrateInstance6 -D` *rootDN* `-w` *password* `-p` *port* `-o` *oldInstancePath* `-n` *newInstancePath*

   where:

- *rootDN* is the Directory Server 6.x user DN with *root* permissions, such as `Directory Manager`.
- *password* is the password for `Directory Manager` in Directory Server 6.x.
- *port* is the LDAP port number assigned to Directory Server 6.x.
- *oldInstancePath* is the path to the installation directory of the legacy Directory Server (for example, `/usr/netscape/server4/slapd-`*serverID*).
- *newInstancePath* is the path to the installation directory of Directory Server 6.x (for example, `/usr/netscape/servers/slapd-`*serverID*).

The following is an example of a command you would use on a UNIX machine to migrate an instance of Directory Server 4.11 to Directory Server 6.x:

```
migrateInstance6 -D "cn=Directory Manager" -w secret -p 1389
-o /usr/netscape/server4/slapd-phonebook
-n /usr/netscape/servers/slapd-phonebook
```

The following is an example of the same command on a Windows machine:

```
perl migrateInstance6 -D "cn=Directory Manager" -w secret -p 1389
-o c:\netscape\server4\slapd-phonebook
-n c:\netscape\servers\slapd-phonebook
```

4. Follow the prompts. For example, if you're prompted to provide a path and filename for your backup directory, enter one or accept the default.

   The migration process starts. At the end of migration, your legacy Directory Server is migrated. Additionally, as a result of this migration: a new Directory Server 6.x instance is installed using the configuration information obtained from your legacy Directory Server; the data from your old server is migrated to the new server; and the new server is started.

   A sample output showing migration of Directory Server 5.0 to Directory Server 6.1 is provided below. Notice that the script detects three backends, `backend1`, `backend2`, and `userRoot`, which exist in the legacy server as well as in the new server instances. To demonstrate the various options, for each backend a different option was chosen: for `backend1`, the choice was to continue with the migration and export processes; for `backend2`, the choice was to continue with the migration process only (without exporting); and for `userRoot`, the choice was to skip the migration process.

```
migrate5to6 -D "cn=directory manager" -w secret12 -p 11440 -o
/export/home/jdoe/50-latest/slapd-bart -n
/export/home/jdoe/61-latest/slapd-bart -t 3 -L log.out

oldDir: /export/home/jdoe/50-latest,
```

```
oldHome:/export/home/jdoe/50-latest/slapd-bart,
oldConfDir: /export/home/jdoe/50-latest/slapd-bart/config/,
ldif_rep: /export/home/jdoe/50-latest/slapd-bart/config//ldif/,

rootDN: cn=directory manager,
Port: 11440,
Newname: bart


Shutdown the legacy Directory Server instance:
/usr/netscape/servers/ds50/slapd-bart

Shutting down server slapd-bart . . .

. . .

Name of the old LDAP server: bart.netscape.com
Name of the new LDAP server: bart.netscape.com
6.0 localuser: jdoe, uid: 9871, gid: 10
5.x localuser: jdoe, uid: 9871, gid: 10

Backup /export/home/jdoe/61-latest/slapd-bart/config on
/export/home/jdoe/61-latest/slapd-bart/config_backup ...

Where do you want to back up your configuration directory
[/export/home/jdoe/61-latest/slapd-bart/config_backup] ?

Migrate the schema...

Connected to 6.1 LDAP server

------------------------------------------------------------------------

Parse the old DSE ldif file:
/export/home/jdoe/50-latest/slapd-bart/config/dse.ldif  *****

This may take a while ...


Migrate DSE entries...

SECURITY - Update successfull: cn=encryption,cn=config
SNMP - Update successfull: cn=snmp,cn=config

Compared to the old instance, the current new plugin cn=referential
integrity postoperation,cn=plugins,cn=config belongs this attribute:
nsslapd-pluginarg7

Param: nstransmittedcontrols values To migrate: 2.16.840.1.113730.3.4.2
2.16.840.1.113730.3.4.9 1.2.840.113556.1.4.473 1.3.6.1.4.1.1466.29539.12
Param: nstransmittedcontrols new current values: 2.16.840.1.113730.3.4.2
2.16.840.1.113730.3.4.9 1.2.840.113556.1.4.473 1.3.6.1.4.1.1466.29539.12
```

```
Param: nsslapd-timelimit values To migrate: 3600
Param: nsslapd-timelimit new current values: 3600
Param: nsconcurrentbindlimit values To migrate: 10
Param: nsconcurrentbindlimit new current values: 10
Param: nsbindconnectionslimit values To migrate: 3
Param: nsbindconnectionslimit new current values: 3
Param: nsconnectionlife values To migrate: 0
Param: nsconnectionlife new current values: 0
Param: nsbindretrylimit values To migrate: 3
Param: nsbindretrylimit new current values: 3
Param: nsoperationconnectionslimit values To migrate: 10
Param: nsoperationconnectionslimit new current values: 10
Param: nsreferralonscopedsearch values To migrate: off
Param: nsreferralonscopedsearch new current values: off
Param: nsmaxtestresponsedelay values To migrate: 15
Param: nsmaxtestresponsedelay new current values: 15
Param: nsmaxresponsedelay values To migrate: 60
Param: nsmaxresponsedelay new current values: 60
Param: nsbindtimeout values To migrate: 15
Param: nsbindtimeout new current values: 15
Param: nsabandonedsearchcheckinterval values To migrate: 2
Param: nsabandonedsearchcheckinterval new current values: 2
Param: nsconcurrentoperationslimit values To migrate: 10
Param: nsconcurrentoperationslimit new current values: 10
Param: nschecklocalaci values To migrate: off
Param: nschecklocalaci new current values: off
Param: nshoplimit values To migrate: 10
Param: nshoplimit new current values: 10
Param: nsslapd-sizelimit values To migrate: 2000
Param: nsslapd-sizelimit new current values: 2000
Param: nsproxiedauthorization values To migrate: on
Param: nsproxiedauthorization new current values: on

------------------------------------------------------------------------

Migrate LDBM backend instances...


*** LDBM_BACKEND_INSTANCE - cn=backend1,cn=ldbm database,cn=plugins,cn=config
already exists

*** Migration will overwrite existing database
Do you want to continue Yes/No [No] ? y
Do you want to export the existing data Yes/No [Yes] ?

Enter the full pathname of the file
[/export/home/jdoe/61-latest/slapd-bart/db_backup/backend1.ldif]:
```

```
Existing data will be exported under
/export/home/jdoe/61-latest/slapd-bart/db_backup/backend1.ldif

Continue Yes/No [No] ? y

Now baking up database backend1 in
/export/home/jdoe/61-latest/slapd-bart/db_backup/backend1.ldif

Shutting down server slapd-bart . . .

 ldiffile: /export/home/jdoe/61-latest/slapd-bart/db_backup/backend1.ldif
 [12/Jun/2002:10:32:05 -0700] - export backend1: Processed 3 entries (100%).
 [12/Jun/2002:10:32:05 -0700] - Waiting for 4 database threads to stop
 [12/Jun/2002:10:32:07 -0700] - All database threads now stopped

try to reconnect to search cn=backend2,cn=ldbm database,cn=plugins,cn=config


*** LDBM_BACKEND_INSTANCE - cn=backend2,cn=ldbm database,cn=plugins,cn=config
already exists

*** Migration will overwrite existing database

Do you want to continue Yes/No [No] ? y
Do you want to export the existing data Yes/No [Yes] ? n

We should add the backend instance cn=backend3,cn=ldbm
database,cn=plugins,cn=config

LDBM_BACKEND_INSTANCE - Add successfull: cn=backend3,cn=ldbm
database,cn=plugins,cn=config


*** INFORMATION - NetscapeRoot is NOT migrated


*** LDBM_BACKEND_INSTANCE - cn=userroot,cn=ldbm database,cn=plugins,cn=config
already exists

*** Migration will overwrite existing database

Do you want to continue Yes/No [No] ?

*** Migration will not update it

------------------------------------------------------------------------

Migrate mapping tree...
```

```
*** MAPPING_TREE - cn="dc=backend1,dc=com",cn=mapping tree,cn=config already
exists
*** Migration will not add the suffix
*** MAPPING_TREE - cn="dc=backend2,dc=com",cn=mapping tree,cn=config already
exists
*** Migration will not add the suffix

MAPPING_TREE - Add successfull: cn="dc=backend3,dc=com",cn=mapping tree,cn=config
*** MAPPING_TREE - cn="dc=netscape,dc=com",cn=mapping tree,cn=config already
exists
*** Migration will not add the suffix

-------------------------------------------------------------------------

Migrate default indexes...

-------------------------------------------------------------------------

Migrate indexes...

-------------------------------------------------------------------------

Migrate replicas...

-------------------------------------------------------------------------

Migrate replication agreements...

-------------------------------------------------------------------------

Migrate key/cert databases...

-------------------------------------------------------------------------

Migrate Certmap.conf...

Where do you want to back up the file
/export/home/jdoe/61-latest/shared/config/certmap.conf
[/export/home/jdoe/61-latest/shared/config/certmap.conf_backup] ?


***** Close the LDAP connection to the new Directory Server instance *****
Shutting down server slapd-bart . . .

. . .

-------------------------------------------------------------------------

Data processing...

ldiffile: /export/home/jdoe/50-latest/slapd-bart/config//ldif/backend1.ldif
 [12/Jun/2002:10:33:25 -0700] - export backend1: Processed 3 entries (100%).
 [12/Jun/2002:10:33:25 -0700] - Waiting for 2 database threads to stop
 [12/Jun/2002:10:33:26 -0700] - All database threads now stopped
```

```
ldiffile: /export/home/jdoe/50-latest/slapd-bart/config//ldif/backend2.ldif
 [12/Jun/2002:10:33:29 -0700] - export backend2: Processed 3 entries (100%).
 [12/Jun/2002:10:33:29 -0700] - Waiting for 1 database threads to stop
 [12/Jun/2002:10:33:30 -0700] - All database threads now stopped

ldiffile: /export/home/jdoe/50-latest/slapd-bart/config//ldif/backend3.ldif
 [12/Jun/2002:10:33:32 -0700] - export backend3: Processed 2 entries (100%)
 [12/Jun/2002:10:33:32 -0700] - Waiting for 1 database threads to stop
 [12/Jun/2002:10:33:33 -0700] - All database threads now stopped

 Done.
 [12/Jun/2002:10:33:37 -0700] - import backend1: Index buffering enabled with
 bucket size 15
 [12/Jun/2002:10:33:37 -0700] - import backend1: Beginning import job...
 [12/Jun/2002:10:33:37 -0700] - import backend1: Processing file

"/export/home/jdoe/50-latest/slapd-bart/config//ldif/backend1.ldif"
 [12/Jun/2002:10:33:37 -0700] - import backend1: Finished scanning file
"/export/home/jdoe/50-latest/slapd-bart/config//ldif/backend1.ldif" (3 entries)
 [12/Jun/2002:10:33:40 -0700] - import backend1: Cleaning up producer thread...
 [12/Jun/2002:10:33:40 -0700] - import backend1: Indexing complete.
Post-processing...
 [12/Jun/2002:10:33:40 -0700] - import backend1: Flushing caches...
 [12/Jun/2002:10:33:40 -0700] - import backend1: Closing files...
 [12/Jun/2002:10:33:40 -0700] - import backend1: Import complete.  Processed 3
 entries in 3 seconds. (1.00 entries/sec)
 [12/Jun/2002:10:33:44 -0700] - import backend2: Index buffering enabled with
 bucket size 15
 [12/Jun/2002:10:33:44 -0700] - import backend2: Beginning import job...
 [12/Jun/2002:10:33:44 -0700] - import backend2: Processing file
"/export/home/jdoe/50-latest/slapd-bart/config//ldif/backend2.ldif"
 [12/Jun/2002:10:33:44 -0700] - import backend2: Finished scanning file
"/export/home/jdoe/50-latest/slapd-bart/config//ldif/backend2.ldif" (3 entries)
 [12/Jun/2002:10:33:44 -0700] - import backend2: Workers finished; cleaning up...
 [12/Jun/2002:10:33:47 -0700] - import backend2: Workers cleaned up.
 [12/Jun/2002:10:33:47 -0700] - import backend2: Cleaning up producer thread...
 [12/Jun/2002:10:33:47 -0700] - import backend2: Indexing complete.
Post-processing...
 [12/Jun/2002:10:33:47 -0700] - import backend2: Flushing caches...
 [12/Jun/2002:10:33:47 -0700] - import backend2: Closing files...
 [12/Jun/2002:10:33:47 -0700] - import backend2: Import complete.  Processed 3
 entries in 3 seconds. (1.00 entries/sec)
 [12/Jun/2002:10:33:50 -0700] - import backend3: Index buffering enabled with
 bucket size 15
 [12/Jun/2002:10:33:50 -0700] - import backend3: Beginning import job...
 [12/Jun/2002:10:33:51 -0700] - import backend3: Processing file
"/export/home/jdoe/50-latest/slapd-bart/config//ldif/backend3.ldif"
```

```
 [12/Jun/2002:10:33:51 -0700] - import backend3: Finished scanning file
"/export/home/jdoe/50-latest/slapd-bart/config//ldif/backend3.ldif" (2 entries)
 [12/Jun/2002:10:33:51 -0700] - import backend3: Workers finished; cleaning up...
 [12/Jun/2002:10:33:54 -0700] - import backend3: Workers cleaned up.
 [12/Jun/2002:10:33:54 -0700] - import backend3: Cleaning up producer thread...
 [12/Jun/2002:10:33:54 -0700] - import backend3: Indexing complete.
Post-processing...
 [12/Jun/2002:10:33:54 -0700] - import backend3: Flushing caches...
 [12/Jun/2002:10:33:54 -0700] - import backend3: Closing files...
 [12/Jun/2002:10:33:54 -0700] - import backend3: Import complete.  Processed 2
entries in 4 seconds. (0.50 entries/sec)

-----------------------------------------------------------------------

Migrate Changelog...

-----------------------------------------------------------------------

***** Migrate ReplicaBindDN entries...

-----------------------------------------------------------------------

***** Migrate MultiplexorBindDN entries...


  ******   End of migration   ******
```

Migrating a 4.x Replicated Site

The procedure described in this section explains the migration path that you can follow to migrate a replication topology of 4.x servers to a replication topology of 6.x Directory Servers.

You can migrate instances of Directory Server 4.x because these releases of the Directory Server can replicate to a Directory Server 6.x configured as a consumer. However, the following constraints must be observed in order to successfully complete the migration of a replicated environment:

- The replication topology of legacy servers must be a valid topology.
- The new 6.x Directory Server must be configured as a legacy consumer of the 4.x Directory Server, as explained in Chapter 8, “Managing Replication” of the *Netscape Directory Server Administrator’s Guide*.
- The replication agreement between the 4.x supplier server and the 6.x consumer server must be a 4.x supplier-initiated replication agreement.

The following sections summarize how you can migrate a replicated environment:

- Migrating a Replicated 4.x Site - Approach 1
- Migrating a Replicated 4.x Site - Approach 2

Migrating a Replicated 4.x Site - Approach 1

Given the constraints, an approach to migrating a replication topology of 4.x servers is to:

1. Install the 6.x Directory Server and configure it both:
    - As a read-write replica, the role the server will fulfill once the migration process is completed, that logs changes.
    - As a legacy consumer, the role the server must play during the migration process.
2. Configure the 4.x supplier to send updates to the 6.x Directory Server.
3. Upgrade 4.x consumer servers to Directory Server 6.x, and change their supplier server to be the Directory Server 6.x that you configured in Step 1.

    This Directory Server now acts as a hub supplier.
4. Retire the 4.x supplier.

    The Directory Server 6.x that you configured in Step 1 is now the only supplier in the topology.

To better understand Approach 1, consider a fairly simple replication topology:

- One supplier server, ServerA.
- Two consumer servers, ServerB and ServerC.
- ServerA has a supplier-initiated replication agreement to ServerB and to ServerC.
- ServerA, ServerB, and ServerC are 4.x Directory Servers.

NOTE You can migrate a topology where ServerB and ServerC have consumer initiated replication (CIR) agreements with ServerA. However, you cannot have CIR agreements in the new replication environment because Directory Server 6.x does not support consumer-initiated replication.

To migrate this topology using Approach 1, follow these steps:

1. Install Directory Server 6.x on a new server, ServerD.
2. Configure ServerD for the role it will fulfill in the migrated replication topology, that is as a read-write replica that logs changes.

   This procedure is explained in Chapter 8, "Managing Replication" of the *Netscape Directory Server Administrator's Guide*.
3. Then configure ServerD to be a legacy consumer.

   This procedure is explained in Chapter 8, "Managing Replication" of the *Netscape Directory Server Administrator's Guide*.
4. Migrate ServerB to Directory Server 6.x following the instructions given in "Migrating a Standalone Server" on page 92.
5. Make ServerB a read-only replica of ServerD.

   This means that ServerD is now a hub supplier—it receives updates from ServerA, and in turn updates ServerB.
6. Upgrade ServerC to Directory Server 6.x, and make it a read-only replica of ServerD.
7. Retire ServerA.
8. Disable legacy consumer settings on ServerD.

   This leaves ServerD as the single supplier for consumer ServerB and ServerC.

When you have completed the migration of your replication topology, you can evolve it to use multi-master replication. To do this, you must add a new Directory Server 6.x that acts as a master to your replication topology. You cannot change one of the read-only replicas to become a read-write replica.

For more information on multi-master replication topologies, see Chapter 8, "Managing Replication" of the *Netscape Directory Server Administrator's Guide*.

Migrating a Replicated 4.x Site - Approach 2

Given the constraints, another approach to migrating a replication topology of 4.x servers is to:

1. Shut down all writes to the directory.
2. Migrate the master using the approach given in section "Migrating a Standalone Server" on page 92.
3. At this point, writes may resume to the master.

4. Migrate consumers one at a time. After each migration, recreate migration agreements and re-initialize the migrated consumers.

To better understand Approach 2, consider a fairly simple replication topology:

- One supplier server, ServerA.
- Two consumer servers, ServerB and ServerC.
- ServerA has a supplier-initiated replication agreement to ServerB and to ServerC.
- ServerA, ServerB, and ServerC are 4.x Directory Servers.

NOTE You can migrate a topology where ServerB and ServerC have consumer-initiated replication (CIR) agreements with ServerA. However, you cannot have CIR agreements in the new replication environment because Directory Server 6.x does not support consumer-initiated replication.

To migrate this topology using Approach 2, follow these steps:

1. Migrate Directory Server 6.x on ServerA following the instruction given in section “Migrating a Standalone Server” on page 92.
2. Migrate ServerB to Directory Server 6.x following the instructions given in section “Migrating a Standalone Server” on page 92.
3. Recreate migration agreement between ServerA and ServerB.
4. Re-initialize ServerB.
5. Upgrade ServerC to Directory Server 6.x, and make it a read-only replica of ServerD.
6. Recreate migration agreement between ServerA and ServerC.
7. Re-initialize ServerC.

When you have completed the migration of your replication topology, you can evolve it to use multi-master replication. To do this, you must add a new Directory Server 6.x that acts as a master to your replication topology. You cannot change one of the read-only replicas to become a read-write replica.

For more information on multi-master replication topologies, see Chapter 8, “Managing Replication” of the *Netscape Directory Server Administrator’s Guide*.

Migrating a 5.x Replicated Site

If you are upgrading from Directory Server 5.x to Directory Server 6.x, your replication configuration is automatically migrated when you run the `migrateInstance6` script.

To migrate a 5.x replicated site:

1. Stop your Directory Server 5.x.
2. Install Directory Server 6.x.
3. Run the migration script as shown in section “Migrating a Standalone Server” on page 92.
4. Once your 5.x server is migrated, test replication and make sure it is working correctly.
5. After you finish this process for the master, repeat the steps for the consumers.

Migrating a 5.x Multi-Master Deployment

This section explains how to migrate a live multi master replication (MMR) architecture built using Directory Server 5.x to Directory Server 6.x in a production environment. The procedure outlined here ensures that your environment will stay live and no re-initialization will be needed.

The instructions are written with these assumptions:

- Your deployment consists of separate configuration and standard access instances of Directory Server.
- You are upgrading to Directory Server 6.2.

The migration process can be summarized into these steps:

1. Stop directory writes on both masters.

   It is imperative that there are no entries being written or changed on the masters during the migration. After both the masters are migrated, writes can resume.

2. After stopping provisioning, make sure all changes have been replicated from the server to migrate to all of its consumers.

   Any changes left over in the `changelog` will be lost after migration, so make sure all changes in the `changelog` have been replicated to all consumers.

3. Migrate the first master; see section “Master Migration” on page 104.
4. Verify that writes and changes are being replicated through the servers.
5. Migrate the second master; see section “Master Migration” on page 104.
6. Verify that writes and changes are being replicated through the servers.
7. Migrate the hubs (if any); see section “Hub Migration” on page 104.
8. Verify that writes and changes are being replicated through the servers.
9. Migrate the consumers; see section “Consumer Migration” on page 105.
10. Verify that writes and changes are being replicated through the servers.

Master Migration

Follow these steps for the first master and then, repeat the steps for the second:

1. Stop the 5.x Directory Server.
2. Install Directory Server 6.x.

   Make this your configuration instance, as it is not replicated. For the second master, register against the first master’s configuration instance.
3. Log into console and create a new instance that you are going to migrate to.

   This instance will need to be created to listen on the port that your standard access will be to (usually 389).
4. Run the migration script following the instruction in “Migrating a Standalone Server” on page 92.
5. Once your master is migrated, test replication and make sure that it is working correctly.
6. After you finish this process for the first master, repeat the steps for the second master.

   You may wish to set up multi-master replication for `o=NetscapeRoot` between the instances on the masters.

Hub Migration

To migrate a 5.x hub:

1. Stop your Directory Server 5.x.

2. Install Directory Server 6.x, registering against the first master's configuration instance.
3. Run the migration script following the instructions in "Migrating a Standalone Server" on page 92.
4. Once your hub is migrated, test replication and make sure that it is working correctly.
5. After you finish this process for the first hub, repeat the steps for any additional hubs.

Consumer Migration

To migrate a 5.x consumer server:

1. Stop the 5.x Directory Server.
2. Install Directory Server 6.x, registering against the first master's configuration instance.
3. Run the migration script; see section "Migrating a Standalone Server" on page 92.
4. Once your consumer is migrated, test replication and make sure that it is working correctly.
5. After you finish this process for the first consumer, repeat the steps for any additional consumers.

Managing Console Fail Over

If you have a multi-master installation with `o=NetscapeRoot` replicated between your two masters, Server1 and Server2, you can modify the console on the second server (Server2) so that it uses Server2's instance instead of Server1's. (By default, writes with Server2's console would be made to Server1 then replicated over.)

To accomplish this, you must:

1. Shut down the Administration Server and Directory Server.
2. Change these files to reflect Server2's values:

   serverRoot`/userdb/dbswitch.conf:directory default ldap://`*configHostname*`:`*configPort*`/o%3DNetscapeRoot`

   serverRoot`/admin-serv/config/adm.conf:ldapHost:` *configHostname*
   serverRoot`/admin-serv/config/adm.conf:ldapPort:` *configPort*

serverRoot/shared/config/dbswitch.conf:directory default ldap://*configHostname*:*configPort*/o%3DNetscapeRoot

serverRoot/slapd-*serverID*/config/dse.ldif:nsslapd-pluginarg0: ldap://*configHostname*:*configPort*/o%3DnetscapeRoot

3. Turn off the pass through authentication (PTA) plug-in on Server2 by editing its dse.ldif file.
   a. In a text editor, open this file:

      serverRoot/slapd-*serverID*/config/dse.ldif

   b. Locate the entry for the PTA plug-in:

      dn: cn=Pass Through Authentication,cn=plugins,cn=config

   c. Change nsslapd-pluginEnabled: on to nsslapd-pluginEnabled: off.
4. Restart the Directory Server and Administration Server.

Upgrading From Directory Server 6.x Versions

You can upgrade an instance of Directory Server 6.0x or 6.1x (for example, 6.0, 6.01, 6.02, 6.1, or 6.11) to Directory Server 6.2 by installing Directory Server 6.2 into the same installation directory in which your 6.0x or 6.1x Directory Server instance is installed. These sections explain the upgrade process:

- Before You Begin
- Upgrading
- After You Upgrade

Before You Begin

Before you begin the upgrade process, back up your entire 6.0x or 6.1x Directory Server. For instructions, check *backing up* and *exporting* related topics in Chapter 4, “Populating Directory Databases” of the *Netscape Directory Server Administrator’s Guide*.

Upgrading

The steps below show how to perform an upgrade using the Typical mode of installation on UNIX:

1. On your Directory Server 6.0x or 6.1x host machine, log in as `root` or superuser (`su`).
2. Stop the server.

   # *serverRoot*`/slapd-`*serverID*`/stop-server`
3. Create a new directory, for example:

   ```
   # mkdir ds62
   # cd ds62
   ```
4. Download the Directory Server product binaries file to the directory you created.
5. Unpack the product binaries file using the following command:

   `# gunzip -dc` *filename*`.tar.gz | tar -xvof -`

   where *filename* corresponds to the product binaries that you want to unpack.
6. In the list of files, locate the `setup` program.
7. Run the `setup` program by issuing the following command (from the installation directory):

   `./setup`

   The `setup` program asks if you would like to proceed with the setup.
8. Press Enter to respond with the default (the default for this prompt is Yes) or press `n` if you would like to exit the `setup` program.

   (If you want to log in as `root` or superuser (use the `su` command), you will need to exit the `setup` program.)
9. Next, the `setup` program asks you if you agree to the license terms. Press `y` to agree with the license terms.
10. When you are asked what you would like to install, press Enter to select the default, Netscape Servers.
11. When you are asked what type of installation you would like to perform, press Enter to select the default, Typical Installation.

12. When prompted to enter the server root (or the installation directory), enter the full path to the location where your Directory Server 6.0x or 6.1x is installed.

    By default, the `setup` program provides the following path:

    `/usr/netscape/servers`

    If your 6.0x or 6.1x Directory Server is installed in a different path, be sure to select that path. Once you supply the correct path, press Enter.

13. The `setup` program starts upgrading your server. Follow the prompts and complete the upgrade process.

14. Restart the server.

    `#` *serverRoot*`/slapd-`*serverID*`/stop-server`

After You Upgrade

To verify that the upgrade process was successful, it is recommended that you check the upgraded server for data consistency and any custom schema.

Chapter 7

Uninstalling Directory Server

You may need to remove an instance of Netscape Directory Server (Directory Server) or uninstall the entire server altogether. The Directory Server provides a utility that enables you to uninstall the software as a whole or to remove selected components. This chapter explains how to perform these tasks in these sections:

- Removing a Directory Server Instance (page 109)
- Uninstalling Directory Server (page 110)

Removing a Directory Server Instance

If you are sure you won't need a particular instance of the Directory Server anymore, you can use the Netscape Console to remove the server instance from your machine. Removing a Directory Server instance is not the same as uninstalling the Directory Server: when you uninstall the Directory Server, its program files are deleted from the host machine; when you remove a Directory Server instance, only the selected instance is removed, leaving behind the configuration directory and Administration Server because you require these to administer the remaining server instances installed in the server group.

NOTE Before removing an instance of Directory Server, verify that the corresponding *configuration directory* is running.

To remove a Directory Server instance from your machine:

1. Log in to Netscape Console.
2. In the Console tab, select the Directory Server instance you want to remove.

3. From the Object menu, select Stop; you can also right-click to choose this option from the pop-up menu.
4. When the server has stopped, from the Object menu, choose Remove Server.

   You can also right-click to choose this option from the pop-up menu.
5. When prompted, confirm that you want to remove the server instance.

Uninstalling Directory Server

To uninstall Directory Server from a machine, use the uninstallation utility. To remove a specific instance of Directory Server, follow the instructions provided in “Removing a Directory Server Instance,” on page 109.

The sections that follow provide instructions for:

- Uninstalling the Server on UNIX Systems
- Uninstalling Directory Server on Windows Systems

CAUTION You will not receive a warning before proceeding with the uninstallation of the Directory Server which contains your configuration information under the `o=NetscapeRoot` suffix.

The configuration Directory Server containing the `o=NetscapeRoot` suffix contains the configuration data for your deployment, and should not therefore be uninstalled before dependent Directory Servers. It is the first Directory Server you install and we strongly recommend that it be the last one you uninstall.

Uninstalling the Server on UNIX Systems

To uninstall Directory Server running on a UNIX system:

1. Log in to your system as super user (root).
2. Navigate to the directory where Directory Server is installed.

   The default path is `/usr/netscape/servers`.
3. Run `./uninstall`.

4. Select the default, `All`, to remove all components of Directory Server.

   Alternately, you may choose to remove individual components by selecting them from the list that appears on the screen:

   - Administration Services
   - Netscape Directory Suite
   - Server Core Components
   - nsPerl
   - PerLDAP

5. When prompted, enter the administrator ID and password for the configuration directory to authorize removal of Directory Server.

   The uninstallation utility starts removing files. After the utility has finished removing files, a message is displayed indicating that some files have not been removed from your system.

6. Go to the installation directory, and manually remove any remaining files to complete the uninstallation process.

   Be sure to check the `\tmp\install.log` file for details about the uninstallation process.

Uninstalling Directory Server on Windows Systems

There are two ways in which you can uninstall Directory Server from a Windows system:

- Using Directory Server's Uninstall Utility
- Using Windows Add/Remove Programs Utility

Using Directory Server's Uninstall Utility

To uninstall Directory Server from your Windows system using the `uninst.exe` utility:

1. Log in to your system as administrator.
2. Navigate to the directory where Directory Server is installed.

   The default path is `c:\netscape\servers`.

3. Locate and double-click the uninstallation utility, `uninst.exe`.

   The Netscape Uninstall window appears, showing a list of components:

   - Administration Services
   - Netscape Directory Suite
   - Server Core Components
   - nsPerl
   - PerLDAP

4. Select the components you want to remove and click Uninstall.

   To remove specific subcomponents, select the component and click Sub Components. This will open a list of subcomponents of the selected component. Select the desired subcomponents and click Continue.

   Note that certain components have dependencies on other components and cannot be removed without selecting both components. If you select a component that has a dependency on another that was not selected, an error message will appear instructing you to select that component.

5. When prompted, enter the configuration administrator ID and password and click OK to authorize removal of files.

   The uninstallation utility starts removing files. After the utility has finished removing files, a message is displayed indicating that some files have not been removed from your system.

6. Go to the installation directory, and manually remove any remaining files to complete the uninstallation process.

   Be sure to check the `c:\temp\Install.log` file for details about the uninstallation process.

Using Windows Add/Remove Programs Utility

To uninstall Directory Server using the Add/Remove Programs utility:

1. From the Start menu, choose Settings, then Control Panel.
2. Double-click Add/Remove Programs.

   The Add/Remove Programs Properties window opens.

3. Locate and select the entry for Netscape Directory Server.

   The entry is of the form `Netscape Server Products` *version_number server_root*, where *version_number* is your Directory Server's version number and *server_root* is your Directory Server's installation directory.

4. Click Add/Remove.

   The Netscape Uninstall window appears, showing a list of components:

   - Administration Services
   - Netscape Directory Suite
   - Server Core Components
   - nsPerl
   - PerLDAP

5. Select the components you want to remove and click Uninstall.

   To remove specific subcomponents, select the component and click Sub Components. This will open a list of subcomponents of the selected component. Select the desired subcomponents and click Continue.

   Note that certain components have dependencies on other components and can not be removed without selecting both components. If you select a component that has a dependency on another that was not selected, an error message will appear instructing you to select that component.

6. When prompted, enter the configuration administrator ID and password and click OK to authorize removal of files.

   The uninstallation utility starts removing files. After the utility has finished removing files, a message is displayed indicating that some files have not been removed from your system.

7. Go to the installation directory, and manually remove any remaining files to complete the uninstallation process.

   Be sure to check the `c:\temp\Install.log` file for details about the uninstallation process.

Chapter 8

Troubleshooting

This chapter describes the most common installation problems and how to solve them. It also provides some tips on checking patch levels and kernel parameter settings for your system.

This chapter has the following sections:

- Running dsktune (page 115)
- Common Installation Problems (page 119)

Running dsktune

The `dsktune` utility provides an easy and reliable way of checking the patch levels and kernel parameter settings for your system. You must install the Directory Server before you can run `dsktune`. `dsktune` is not available for Windows platform.

On Solaris platform, if you run the `dsktune` utility, you need to be aware that it will report as missing any of the patches from the Sun recommended patch list that are not installed on your system, even if they relate to packages that you have not installed.

To run `dsktune`:

1. Change to the installation directory for your Directory Server.

   By default, this directory is `/usr/netscape/servers`.

2. Change to the `bin/slapd/server` subdirectory.

3. As root, enter the following command:

   ```
   # ./dsktune
   ```

The following is an example of output that dsktune generates. Note that dsktune does not itself make any changes to the system.

```
Netscape Directory Server system tuning analysis version 15-MAY-2003.

NOTICE : System is usparc-SUNW,Ultra-5_10-solaris5.8_s28s_u7wos_08a (1
processor).

ERROR : Patch 108528-18 is present, but 108528-19 (Feb/21/2003: SunOS 5.8:
kernel update patch) is a more recent version.

ERROR : Patch 108727-19 is present, but 108727-22 (Feb/21/2003: SunOS 5.8:
/kernel/fs/nfs and /kernel/fs/sparcv9/nfs patch) is a more recent version.

ERROR : Patch 108827-35 is present, but 108827-40 (Feb/07/2003: SunOS 5.8:
/usr/lib/libthread.so.1 patch) is a more recent version.

ERROR : Patch 108919-15 is present, but 108919-16 (Jan/31/2003: CDE 1.4:
dtlogin patch) is a more recent version.

ERROR : Patch 108968-07 is present, but 108968-08 (Jan/22/2003: SunOS 5.8:
vol/vold/rmmount/dev_pcmem.so.1 patch) is a more recent version.

ERROR : Patch 108993-12 is present, but 108993-13 (Jan/30/2003: SunOS 5.8: nss
and ldap patch) is a more recent version.

ERROR : Patch 109007-08 is present, but 109007-09 (Jan/27/2003: SunOS 5.8:
at/atrm/batch/cron patch) is a more recent version.

ERROR : Patch 109318-28 is present, but 109318-31 (Feb/07/2003: SunOS 5.8:
suninstall Patch) is a more recent version.

ERROR : Patch 109326-09 is present, but 109326-10 (Feb/03/2003: SunOS 5.8:
libresolv.so.2 and in.named patch) is a more recent version.

ERROR : Patch 109805-14 is present, but 109805-15 (Jan/23/2003: SunOS 5.8:
/usr/lib/security/pam_krb5.so.1 patch) is a more recent version.

ERROR : Patch 109888-18 is present, but 109888-20 (Feb/21/2003: SunOS 5.8:
platform drivers patch) is a more recent version.

ERROR : Patch 110453-03 is present, but 110453-04 (Feb/21/2003: SunOS 5.8:
admintool Patch) is a more recent version.

ERROR : Patch 110842-08 is present, but 110842-10 (Feb/06/2003: SunOS 5.8:
hpc3130 driver patch for SUNW,Sun-Fire-880) is a more recent version.
```

```
ERROR : Patch 110934-10 is present, but 110934-11 (Feb/20/2003: SunOS 5.8:
pkgtrans, pkgadd, pkgchk and libpkg.a patch) is a more recent version.

ERROR : Patch 111874-05 is present, but 111874-06 (Jan/23/2003: SunOS 5.8:
usr/bin/mail patch) is a more recent version.

ERROR  : Patch 111879-01 (Aug/27/2001: SunOS 5.8: Solaris Product Registry
patch SUNWwsr) is required but not installed.

ERROR : Patch 112237-06 is present, but 112237-07 (Jan/15/2003: SunOS 5.8:
mech_krb5.so.1 patch) is a more recent version.

ERROR  : Patch 113650-01 (Jan/08/2003: SunOS 5.8: /usr/lib/utmp_update patch)
is required but not installed.

NOTICE : Solaris patches can be obtained from http://sunsolve.sun.com or your
Solaris support representative.  Solaris patches listed as required by the
JRE are located at http://www.sun.com/software/solaris/jre/download.html or
can be obtained from your Solaris support representative.

WARNING: 384MB of physical memory is available on the system. 1024MB is
recommended for best performance on large production system.

WARNING: This program should be run by the superuser to collect kernel
information on the overriding maximum backlog queue size and IP tuning.

WARNING: The tcp_close_wait_interval is set to 240000 milliseconds
(240 seconds).  This value should be reduced to allow for more
simultaneous connections to the server.  A line similar to the following
should be added to the /etc/init.d/inetinit file:
ndd -set /dev/tcp tcp_time_wait_interval 30000

NOTICE : The tcp_conn_req_max_q value is currently 128, which will limit the
value of listen backlog which can be configured.  It can be raised by adding
to /etc/init.d/inetinit, after any adb command, a line similar to:
ndd -set /dev/tcp tcp_conn_req_max_q 1024

NOTICE : The tcp_keepalive_interval is set to 7200000 milliseconds
(120 minutes).  This may cause temporary server congestion from lost
client connections.

NOTICE : The tcp_keepalive_interval can be reduced by adding the following line
to /etc/init.d/inetinit:
ndd -set /dev/tcp tcp_keepalive_interval 600000
```

```
NOTICE : The NDD tcp_rexmit_interval_initial is currently set to 3000
milliseconds (3 seconds).  This may cause packet loss for clients on
Solaris 2.5.1 due to a bug in that version of Solaris.  If the clients are not
using Solaris 2.5.1, no problems should occur.

NOTICE : If the directory service is intended only for LAN or private
high-speed WAN environment, this interval can be reduced by adding to
/etc/init.d/inetinit:
ndd -set /dev/tcp tcp_rexmit_interval_initial 500

NOTICE : The NDD tcp_ip_abort_cinterval is currently set to 180000
milliseconds (180 seconds).  This may cause long delays in establishing
outgoing connections if the destination server is down.

NOTICE : If the directory service is intended only for LAN or private
high-speed WAN environment, this interval can be reduced by adding to
/etc/init.d/inetinit:
ndd -set /dev/tcp tcp_ip_abort_cinterval 10000

NOTICE : The NDD tcp_ip_abort_interval is currently set to 180000
milliseconds (180 seconds).  This may cause long delays in detecting
connection failure if the destination server is down.

NOTICE : If the directory service is intended only for LAN or private
high-speed WAN environment, this interval can be reduced by adding to
/etc/init.d/inetinit:
ndd -set /dev/tcp tcp_ip_abort_interval 60000

NOTICE : The NDD tcp_smallest_anon_port is currently 32768.  This allows a
maximum of 32768 simultaneous connections.  More ports can be made available by
adding a line to /etc/init.d/inetinit:
ndd -set /dev/tcp tcp_smallest_anon_port 8192

WARNING: tcp_deferred_ack_interval is currently 100 milliseconds. This will
cause Solaris to insert artificial delays in the LDAP protocol.  It should
be reduced during load testing.
This line can be added to the /etc/init.d/inetinit file:
ndd -set /dev/tcp tcp_deferred_ack_interval 5

WARNING: There are only 1024 file descriptors (hard limit) available, which
limit the number of simultaneous connections.  Additional file descriptors,
up to 65536, are available by adding to /etc/system a line like
set rlim_fd_max=4096
```

```
WARNING: There are only 256 file descriptors (soft limit) available, which
limit the number of simultaneous connections.  Additional file descriptors,
up to 1024 (hard limit), are available by issuing 'ulimit' ('limit' for tcsh)
command with proper arguments.
ulimit -n 4096

ERROR  : The above errors MUST be corrected before proceeding.
```

Common Installation Problems

Clients cannot locate the server.

First, try using the host name. If that does not work, use the fully qualified name (such as `www.domain.com`), and make sure the server is listed in the DNS. If that does not work, use the IP address.

If your NIS domain is different from your DNS domain, the fully qualified host and domain name presented by the installer may be incorrect. These values must be corrected to use the DNS domain name.

Installation cannot determine the Domain Name for this Host. Your network settings may not be correct, or your host may be on a DHCP network.

Windows 2000 requires setting of domain names in two places, one is the default for the whole computer and the other is the one to use for the specific network connection. If you have not specified the domain name to use for the specific network connection, when installing Directory Server, you will notice the warning message shown below:

```
Setup Warning: Installation cannot determine the Domain Name for
this Host. Your network settings may not be correct, or your host may
be on a DHCP network. If you are using TCP/IP, your Domain Name must
be filed in.

To verify yor Domain Name TCP/IP setting, go to Control Panel
Network Settings, and ensure that your TCP/IP DNS properties have
the Domain Name filled out. Do you want to continue?
```

To avoid this error message:

1. On the desktop, right click the icon labeled My Computer.
2. Click on the Network Identification tab.
3. Click the Properties box.
4. In the Identification Changes dialog box, click More.

5. Next to the label “Primary DNS Suffix of this computer,” enter the appropriate domain name.

The port is in use.

You probably did not shut down a server before you upgraded it. Shut down the old server, then manually start the upgraded one.

Another installed server might be using the port. Make sure the port you have chosen is not already being used by another server.

LDAP authentication error causes install to fail.

If you are installing Directory Server in a network which uses NIS naming rather than DNS naming, you may get the following error:

```
ERROR: Ldap authentication failed for url
ldap://incorrect.DNS.address user id admin (151:Unknown error.)
Fatal Slapd Did not add Directory Server information to
Configuration Server.
ERROR. Failure installing Netscape Directory Server. Do you want
to continue [n]?
```

This error occurs when a machine is not correctly configured to use DNS naming. The default fully qualified host and domain name presented during installation is not correct. If you accept the defaults, you receive the LDAP authentication error.

To successfully install, you need to provide a fully qualified domain name that consists of a local host name along with its domain name. A host name is the logical name assigned to a computer. For example, `mycomputer` is a host name and `example.com` is a fully qualified domain name.

A fully qualified domain name should be sufficient to determine a unique Internet address for any host on the Internet. The same naming scheme is also used for some hosts that are not on the Internet, but share the same namespace for electronic mail addressing.

“Failure (4322): Configuration initialization failed” error message on Linux.

`libjvm.so` (from JRE 1.4), which the Administration Server uses to run servlets requires that the `compat-libstdc++-6.2` package (RPM) be installed when running the server on Redhat 7.x and Advanced Server.

The RPM may or may not be installed depending on the options that were chosen when the operating system was installed. If the RPM is not installed, you will get an error similar to the one shown below.

```
[18/Jun/2002:10:56:39] failure ( 4322): Configuration
initialization failed:

Error running init function load-modules: dlopen of
/export/dstest/bin/https/lib/libNSServletPlugin.so failed

(libstdc++-libc6.1-1.so.2: cannot open shared object file: No
such file or directory)
```

For more information on RPM, check the JRE's release notes at this URL: `http://java.sun.com/j2se/1.4/install-linux.html`

I have forgotten the Directory manager DN and password.

You can find out what the Directory Manager DN is by examining *serverRoot*`/slapd-`*serverID*`/config/dse.ldif` and looking for the `nsslapd-rootdn` attribute.

If you have forgotten the Directory Manager DN password, you can reset it by doing the following:

1. Find the `nsslapd-rootpw` attribute in `slapd.conf`. If the attribute value is not encrypted in any way (that is, it does not start with `{SHA}` or `{CRYPT}`) then the password is exactly what is shown on the parameter.
2. If the attribute is encrypted, then delete the attribute value and replace it with some clear text value. For example, if you change the `nsslapd-rootpw` attribute so that it is:

   ```
   nsslapd-rootpw: my_password
   ```

   then your Directory Manager DN password will be `my_password`.
3. Restart your Directory Server.
4. Once your server has restarted, login as the Directory Manager and change the password. Make sure you select an encryption scheme when you do so.

For information on changing a Directory Manager password, see the *Netscape Directory Server Administrator's Guide.*

Is there a way to debug Directory Server installation and uninstallation problems?

Some problems may develop when you uninstall Directory Server and then reinstall. Logging has been enhanced to report setup and uninstall problems with detailed error messages to provide you with enough information to fix the problem. The setup log file is located in the following path: *serverRoot*`/setup/setup.log`. The uninstall log file, which is named

uninst.log, is stored in the system TEMP directory. On UNIX, this directory is usually /tmp or /var/tmp. On Windows, check the system properties to see the value assigned to the TEMP environment variable (alternatively, you can open a command window and type echo %TEMP%).

Glossary

access control instruction *See ACI.*

ACI Access Control Instruction. An instruction that grants or denies permissions to entries in the directory.

access control list *See ACL.*

ACL Access control list. The mechanism for controlling access to your directory.

access rights In the context of access control, specify the level of access granted or denied. Access rights are related to the type of operation that can be performed on the directory. The following rights can be granted or denied: read, write, add, delete, search, compare, self-write, proxy and all.

account inactivation Disables a user account, group of accounts, or an entire domain so that all authentication attempts are automatically rejected.

All IDs Threshold A size limit which is globally applied to every index key managed by the server. When the size of an individual ID list reaches this limit, the server replaces that ID list with an All IDs token.

All IDs token A mechanism which causes the server to assume that all directory entries match the index key. In effect, the All IDs token causes the server to behave as if no index was available for the search request.

anonymous access When granted, allows anyone to access directory information without providing credentials, and regardless of the conditions of the bind.

approximate index Allows for efficient approximate or “sounds-like” searches.

attribute Holds descriptive information about an entry. Attributes have a label and a value. Each attribute also follows a standard syntax for the type of information that can be stored as the attribute value.

attribute list A list of required and optional attributes for a given entry type or object class.

authenticating directory server In pass-through authentication (PTA), the authenticating directory server is the directory server that contains the authentication credentials of the requesting client. The PTA-enabled host sends PTA requests it receives from clients to the bind host.

authentication (1) Process of proving the identity of the client user to the Directory Server. Users must provide a bind DN and either the corresponding password or certificate in order to be granted access to the directory. Directory Server allows the user to perform functions or access files and directories based on the permissions granted to that user by the directory administrator.

(2) Allows a client to make sure they are connected to a secure server, preventing another computer from impersonating the server or attempting to appear secure when it is not.

authentication certificate Digital file that is not transferable and not forgeable and is issued by a third party. Authentication certificates are sent from server to client or client to server in order to verify and authenticate the other party.

base DN Base distinguished name. A search operation is performed on the base DN, the DN of the entry and all entries below it in the directory tree.

base distinguished name *See base DN*.

bind DN Distinguished name used to authenticate to Directory Server when performing an operation.

bind distinguished name *See bind DN*.

bind rule In the context of access control, the bind rule specifies the credentials and conditions that a particular user or client must satisfy in order to get access to directory information.

branch entry An entry that represents the top of a subtree in the directory.

browser Software, such as Netscape Navigator, used to request and view World Wide Web material stored as HTML files. The browser uses the HTTP protocol to communicate with the host server.

browsing index Otherwise known as the virtual view index, speeds up the display of entries in the Directory Server Console. Browsing indexes can be created on any branchpoint in the directory tree to improve display performance.

CA *See Certificate Authority*.

cascading replication In a cascading replication scenario, one server, often called the hub supplier acts both as a consumer and a supplier for a particular replica. It holds a read-only replica and maintains a change log. It receives updates from the supplier server that holds the master copy of the data, and in turn supplies those updates to the consumer.

certificate A collection of data that associates the public keys of a network user with their DN in the directory. The certificate is stored in within the directory as user object attributes.

Certificate Authority Company or organization that sells and issues authentication certificates. You may purchase an authentication certificate from a Certification Authority that you trust. Also known as a CA.

CGI Common Gateway Interface. An interface for external programs to communicate with the HTTP server. Programs written to use CGI are called CGI programs or CGI scripts, and can be written in many of the common programming languages. CGI programs handle forms or perform output parsing that is not done by the server itself.

chaining A method for relaying requests to another server. Results for the request are collected, compiled and then returned to the client.

change log A change log is record that describes the modifications that have occurred on a replica. The supplier server then replays these modifications on the replicas stored on consumer servers, or on other masters, in the case of multi-master replication.

character type Distinguishes alphabetic characters from numeric or other characters and the mapping of upper-case to lower-case letters.

ciphertext Encrypted information that cannot be read by anyone without the proper key to decrypt the information.

CIR *See consumer-initiated replication.*

class definition Specifies the information needed to create an instance of a particular object and determines how the object works in relation to other objects in the directory.

class of service *See CoS.*

classic CoS A classic CoS identifies the template entry by both its DN and the value of one of the target entry's attributes.

client *See LDAP client.*

code page An internal table used by a locale in the context of the internationalization plug-in that the operating system uses to relate keyboard keys to character font screen displays.

collation order Provides language and cultural-specific information about how the characters of a given language are to be sorted. This information might include the sequence of letters in the alphabet or how to compare letters with accents to letters without accents.

consumer Server containing replicated directory trees or subtrees from a supplier server.

consumer-initiated replication Replication configuration where consumer servers pull directory data from supplier servers.

consumer server In the context of replication, a server that holds a replica that is copied from a different server is called a consumer for that replica.

CoS A method for sharing attributes between entries in a way that is invisible to applications.

CoS definition entry Identifies the type of CoS you are using. It is stored as an LDAP subentry below the branch it affects.

CoS template entry Contains a list of the shared attribute values.

daemon A background process on a Unix machine that is responsible for a particular system task. Daemon processes do not need human intervention to continue functioning.

DAP Directory Access Protocol. The ISO X.500 standard protocol that provides client access to the directory.

Data Master The server that is the master source of a particular piece of data.

database link An implementation of chaining. The database link behaves like a database but has no persistent storage. Instead, it points to data stored remotely.

default index One of a set of default indexes created per database instance. Default indexes can be modified, although care should be taken before removing them, as certain plug-ins may depend on them.

definition entry *See CoS definition entry.*

Directory Access Protocol *See DAP.*

directory tree The logical representation of the information stored in the directory. It mirrors the tree model used by most file systems, with the tree's root point appearing at the top of the hierarchy. Also known as DIT.

Directory Manager The privileged database administrator, comparable to the root user in UNIX. Access control does not apply to the directory manager.

Directory Server Gateway (DSGW) A collection of CGI forms that allows a browser to perform LDAP client functions, such as querying and accessing a Directory Server, from a web browser.

directory service A database application designed to manage descriptive, attribute-based information about people and resources within an organization.

distinguished name String representation of an entry's name and location in an LDAP directory.

DIT *See directory tree.*

DM *See Directory Manager.*

DNS Domain Name System. The system used by machines on a network to associate standard IP addresses (such as 198.93.93.10) with hostnames (such as `www.example.com`). Machines normally get the IP address for a hostname from a DNS server, or they look it up in tables maintained on their systems.

DNS alias A DNS alias is a hostname that the DNS server knows points to a different host—specifically a DNS CNAME record. Machines always have one real name, but they can have one or more aliases. For example, an alias such as `www.[yourdomain].[domain]` might point to a real machine called `realthing.[yourdomain].[domain]` where the server currently exists.

DSGW *See Directory Server Gateway (DSGW).*

entry A group of lines in the LDIF file that contains information about an object.

entry distribution Method of distributing directory entries across more than one server in order to scale to support large numbers of entries.

entry ID list Each index that the directory uses is composed of a table of index keys and matching entry ID lists. The entry ID list is used by the directory to build a list of candidate entries that may match the client application's search request.

equality index Allows you to search efficiently for entries containing a specific attribute value.

file extension The section of a filename after the period or dot (.) that typically defines the type of file (for example, .GIF and .HTML). In the filename `index.html` the file extension is `html`.

file type The format of a given file. For example, graphics files are often saved in GIF format, while a text file is usually saved as ASCII text format. File types are usually identified by the file extension (for example, .GIF or .HTML).

filter A constraint applied to a directory query that restricts the information returned.

filtered role Allows you to assign entries to the role depending upon the attribute contained by each entry. You do this by specifying an LDAP filter. Entries that match the filter are said to possess the role.

gateway *See Directory Server Gateway (DSGW).*

general access When granted, indicates that all authenticated users can access directory information.

hostname A name for a machine in the form machine.domain.dom, which is translated into an IP address. For example, `www.example.com` is the machine `www` in the subdomain `example` and `com` domain.

HTML Hypertext Markup Language. The formatting language used for documents on the World Wide Web. HTML files are plain text files with formatting codes that tell browsers such as the Netscape Navigator how to display text, position graphics and form items, and display links to other pages.

HTTP Hypertext Transfer Protocol. The method for exchanging information between HTTP servers and clients.

HTTPD An abbreviation for the HTTP daemon or service, a program that serves information using the HTTP protocol. The daemon or service is often called an httpd.

HTTP-NG The next generation of Hypertext Transfer Protocol.

HTTPS A secure version of HTTP, implemented using the Secure Sockets Layer, SSL.

hub supplier In the context of replication, a server that holds a replica that is copied from a different server, and in turn replicates it to a third server. See also cascading replication.

index key Each index that the directory uses is composed of a table of index keys and matching entry ID lists.

indirect CoS An indirect CoS identifies the template entry using the value of one of the target entry's attributes.

international index Speeds up searches for information in international directories.

International Standards Organization *See ISO.*

IP address Internet Protocol address. A set of numbers, separated by dots, that specifies the actual location of a machine on the Internet (for example, 198.93.93.10).

ISO International Standards Organization

knowledge reference Pointers to directory information stored in different databases.

LDAP Lightweight Directory Access Protocol. Directory service protocol designed to run over TCP/IP and across multiple platforms.

LDAPv3 Version 3 of the LDAP protocol, upon which Directory Server bases its schema format

LDAP client Software used to request and view LDAP entries from an LDAP Directory Server. See also *browser*.

LDAP Data Interchange Format *See LDAP Data Interchange Format.*

LDAP URL Provides the means of locating directory servers using DNS and then completing the query via LDAP. A sample LDAP URL is `ldap://ldap.example.com`

LDBM database A high-performance, disk-based database consisting of a set of large files that contain all of the data assigned to it. The primary data store in Directory Server.

LDIF LDAP Data Interchange Format. Format used to represent Directory Server entries in text form.

leaf entry An entry under which there are no other entries. A leaf entry cannot be a branch point in a directory tree.

Lightweight Directory Access Protocol *See LDAP.*

locale Identifies the collation order, character type, monetary format and time / date format used to present data for users of a specific region, culture, and/or custom. This includes information on how data of a given language is interpreted, stored, or collated. The locale also indicates which code page should be used to represent a given language.

managed object A standard value which the SNMP agent can access and send to the NMS. Each managed object is identified with an official name and a numeric identifier expressed in dot-notation.

managed role Allow you to create an explicit enumerated list of members.

management information base *See MIB.*

mapping tree A data structure that associates the names of suffixes (subtrees) with databases.

master agent *See SNMP master agent.*

matching rule Provides guidelines for how the server compares strings during a search operation. In an international search, the matching rule tells the server what collation order and operator to use.

MD5 A message digest algorithm by RSA Data Security, Inc., which can be used to produce a short digest of data, that is unique with high probability, and is mathematically extremely hard to produce a piece of data that will produce the same message digest.

MD5 signature A message digest produced by the MD5 algorithm.

MIB Management Information Base. All data, or any portion thereof, associated with the SNMP network. We can think of the MIB as a database which contains the definitions of all SNMP managed objects. The MIB has a tree like hierarchy, where the top level contains the most general information about the network and lower levels deal with specific, separate network areas.

MIB namespace Management Information Namespace. The means for directory data to be named and referenced. Also called the directory tree.

monetary format Specifies the monetary symbol used by specific region, whether the symbol goes before or after its value, and how monetary units are represented.

multi-master replication An advanced replication scenario in which two servers each hold a copy of the same read-write replica. Each server maintains a change log for the replica. Modifications made on one server are automatically replicated to the other server. In case of conflict, a time stamp is used to determine which server holds the most recent version.

multiplexor The server containing the database link that communicates with the remote server.

n + 1 directory problem The problem of managing multiple instances of the same information in different directories, resulting in increased hardware and personnel costs.

name collisions Multiple entries with the same distinguished name.

nested role Allow you to create roles that contain other roles.

network management application Network Management Station component that graphically displays information about SNMP managed devices (which device is up or down, which and how many error messages were received, etc.).

network management station *See NMS.*

NIS Network Information Service. A system of programs and data files that Unix machines use to collect, collate, and share specific information about machines, users, file systems, and network parameters throughout a network of computers.

NMS Network Management Station. Powerful workstation with one or more network management applications installed.

ns-slapd Netscape's LDAP Directory Server daemon or service that is responsible for all actions of the Directory Server. See also *slapd*.

object class Defines an entry type in the directory by defining which attributes are contained in the entry.

object identifier A string, usually of decimal numbers, that uniquely identifies a schema element, such as an object class or an attribute, in an object-oriented system. Object identifiers are assigned by ANSI, IETF or similar organizations.

OID *See object identifier.*

operational attributes Operational attributes contain information used internally by the directory to keep track of modifications and subtree properties. They are not returned in response to a search unless explicitly requested.

parent access When granted, indicates that users have access to entries below their own in the directory tree, that is, if the bind DN is the parent of the targeted entry.

pass-through authentication *See PTA.*

pass-through subtree In pass-through authentication, the PTA directory server will pass through bind requests to the authenticating directory server from all clients whose DN is contained in this subtree.

password file A file on Unix machines that stores Unix user login names, passwords, and user ID numbers. It is also known as `/etc/passwd`, because of where it is kept.

password policy A set of rules that govern how passwords are used in a given directory.

permission In the context of access control, the permission states whether access to the directory information is granted or denied, and the level of access that is granted or denied. See access rights.

PDU Protocol Data Unit. Encoded messages which form the basis of data exchanges between SNMP devices.

pointer CoS A pointer CoS identifies the template entry using the template DN only.

presence index Allows you to search for entries that contain a specific indexed attribute.

protocol A set of rules that describes how devices on a network exchange information.

protocol data unit *See PDU.*

proxy authentication A special form of authentication where the user requesting access to the directory does not bind with its own DN but with a proxy DN.

proxy DN Used with proxied authorization. The proxy DN is the DN of an entry that has access permissions to the target on which the client-application is attempting to perform an operation.

PTA Pass-through authentication. Mechanism by which one directory server consults another to check bind credentials.

PTA directory server In pass-through authentication (PTA), the PTA directory server is the server that sends (passes through) bind requests it receives to the authenticating directory server.

PTA LDAP URL In pass-through authentication, the URL that defines the authenticating directory server, pass-through subtree(s) and optional parameters.

RAM Random access memory. The physical semiconductor-based memory in a computer. Information stored in RAM is lost when the computer is shut down.

rc.local A file on Unix machines that describes programs that are run when the machine starts. It is also called `/etc/rc.local` because of its location.

RDN Relative distinguished name. The name of the actual entry itself, before the entry's ancestors have been appended to the string to form the full distinguished name.

referential integrity Mechanism that ensures that relationships between related entries are maintained within the directory.

referral (1) When a server receives a search or update request from an LDAP client that it cannot process, it usually sends back to the client a pointer to the LDAP sever that can process the request.

(2) In the context of replication, when a read-only replica receives an update request, it forwards it to the server that holds the corresponding read-write replica. This forwarding process is called a referral.

replica A database that participates in replication

read-only replica A replica that refers all update operations to read-write replicas. A server can hold any number of read-only replicas.

read-write replica A replica that contains a master copy of directory information and can be updated. A server can hold any number of read-write replicas.

relative distinguished name *See RDN*.

replication Act of copying directory trees or subtrees from supplier servers to consumer servers.

replication agreement Set of configuration parameters that are stored on the supplier server and identify the databases to replicate, the consumer servers to which the data is pushed, the times during which replication can occur, the DN and credentials used by the supplier to bind to the consumer, and how the connection is secured.

RFC Request For Comments. Procedures or standards documents submitted to the Internet community. People can send comments on the technologies before they become accepted standards.

role An entry grouping mechanism. Each role has *members*, which are the entries that possess the role.

role-based attributes Attributes that appear on an entry because it possesses a particular role within an associated CoS template.

root The most privileged user available on Unix machines. The root user has complete access privileges to all files on the machine.

root suffix The parent of one or more sub suffixes. A directory tree can contain more than one root suffix.

schema Definitions describing what types of information can be stored as entries in the directory. When information that does not match the schema is stored in the directory, clients attempting to access the directory may be unable to display the proper results.

schema checking Ensures that entries added or modified in the directory conform to the defined schema. Schema checking is on by default and users will receive an error if they try to save an entry that does not conform to the schema.

Secure Sockets Layer *See SSL.*

self access When granted, indicates that users have access to their own entries, that is, if the bind DN matches the targeted entry.

Server Console Java-based application that allows you to perform administrative management of your Directory Server from a GUI.

server daemon The server daemon is a process that, once running, listens for and accepts requests from clients.

server service The server service is a process on Windows NT that, once running, listens for and accepts requests from clients. It is the SMB server on Windows NT.

server root A directory on the server machine dedicated to holding the server program and configuration, maintenance, and information files.

Server Selector Interface that allows you select and configure servers using a browser.

service A background process on a Windows NT machine that is responsible for a particular system task. Service processes do not need human intervention to continue functioning.

SIE Server Instance Entry, the ID assigned to an instance of Directory Server during installation.

Simple Network Management Protocol *See SNMP.*

single-master replication The most basic replication scenario in which two servers each hold a copy of the same read-write replicas to consumer servers. In a single-master replication scenario, the supplier server maintains a change log.

SIR *See supplier-initiated replication.*

slapd LDAP Directory Server daemon or service that is responsible for most functions of a directory except replication. See also *ns-slapd*.

SNMP Simple Network Management Protocol. Used to monitor and manage application processes running on the servers, by exchanging data about network activity.

SNMP master agent Software that exchanges information between the various subagents and the NMS.

SNMP subagent Software that gathers information about the managed device and passes the information to the master agent.

SSL Secure Sockets Layer. A software library establishing a secure connection between two parties (client and server) used to implement HTTPS, the secure version of HTTP.

standard index Indexes that are maintained by default.

sub suffix A branch underneath a root suffix.

subagent *See SNMP subagent.*

substring index Allows for efficient searching against substrings within entries. Substring indexes are limited to a minimum of two characters for each entry.

suffix The name of the entry at the top of the directory tree, below which data is stored. Multiple suffixes are possible within the same directory. Each database only has one suffix.

superuser The most privileged user available on Unix machines (also called root). The superuser has complete access privileges to all files on the machine.

supplier Server containing the master copy of directory trees or subtrees that are replicated to consumer servers.

supplier server In the context of replication, a server that holds a replica that is copied to a different server is called a supplier for that replica.

supplier-initiated replication Replication configuration where supplier servers replicate directory data to consumer servers.

symmetric encryption Encryption that uses the same key for both encrypting and decrypting. DES is an example of a symmetric encryption algorithm.

system index Cannot be deleted or modified as it is essential to Directory Server operations.

target In the context of access control, the target identifies the directory information to which a particular ACI applies.

target entry The entries within the scope of a CoS.

TCP/IP Transmission Control Protocol / Internet Protocol. The main network protocol for the Internet and for enterprise (company) networks.

template entry *See CoS template entry*.

time / date format Indicates the customary formatting for times and dates in a specific region.

TLS Transport Layer Security. The new standard for secure socket layers, a public key based protocol.

topology The way a directory tree is divided among physical servers and how these servers link with one another.

Transport Layer Security *See TLS*.

uid A unique number associated with each user on a Unix system.

URL Uniform Resource Locator. The addressing system used by the server and the client to request documents. It is often called a location. The format of a URL is `[protocol]://[machine:port]/[document]`. The port number is necessary only on selected servers, and it is often assigned by the server, freeing the user of having to place it in the URL.

virtual list view index Otherwise known as a browsing index, speeds up the display of entries in the Directory Server Console. Virtual list view indexes can be created on any branchpoint in the directory tree to improve display performance.

X.500 standard The set of ISO/ITU-T documents outlining the recommended information model, object classes and attributes used by directory server implementations.

Index

A

administration domain, defined 18
administration port number 28
administration server 12
administration server user 15
authentication entities 15

C

configuration decisions 12
configuration directory administrator 15
configuration directory, defined 16
conventions, in this book 8
creating instances under the same server root 80
creating silent install files 68
custom install, defined 19

D

default server root 13
directory manager 15
directory server 12
directory suffix 16
directory tree
  configuring 84
ds_create 80
dsktune utility 37, 55, 62, 115

E

express install
  defined 19
  using 23

F

fonts, in this book 8

G

glossary of terms 123–138

H

help
  launching 83

I

install.inf 68
installation
  components 11
  configuration decisions 12
  preparing for 11
  process overview 19
    new installations 19
  requirements 33
installation directory, default 14

L

LDAP Data Interchange Format (LDIF)
  creating databases using 84
LDIF, *See* LDAP Data Interchange Format

M

migrating
  4.x replicated sites 99
  5.x MMR deployment 103
  5.x replicated sites 103
  custom schema 90
  standalone server 92
migration 20
  defined 87
  overview 87
  prerequisites 88
  procedure 91

N

Netscape Console 11
netscape root directory tree 16
nobody user account 14
NSHOME 13

O

operating systems 33

P

port numbers
  selecting 13
  troubleshooting 120
preparing for installation 11
PrePreInstall field 37
prerequisites
  migration 88

R

removing the directory server 109
replicated site
  migration of 4.x sites 99
  migration of 5.x MMR deployment 103
  migration of 5.x sites 103
requirements
  computer system 33
root DN (directory manager) 15
running server, users and groups 14

S

schema, migrating 90
server root 13
serverID 8
serverRoot 8
setup program, using from command line 68
silent install
  creating install files 68
  directives 73
    admin 77
    base 78
    nsperl 79

perldap 79
slapd 75
silent install directives
general 74
silent install files 68
silent install, defined 19
silent install, examples 69
typical install 70
silent install, using 67
styles, in this book 8
supported platforms 33

T

terms, in this book 8, 123–138
typical install, defined 19
typical install, using
on NT 29
on UNIX 25

U

uninstalling the directory server 109
upgrade 20
defined 87
upgrading
prerequisites for 106
user and groups to run servers as 14
user directory, defined 17